DIAGNOSTICO E IMPLEMENTACIÓN DE CONTROLES Y MECANISMOS DE SEGURIDAD EN LA RED DE DATOS DE LA ALCALDÍA DE SAN ANTERO CÓRDOBA.

IRINA PADILLA GARCÉS
FRANCISCO JAVIER MOSQUERA ZÚÑIGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGIA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAHAGÚN - CORDOBA
2016

DIAGNOSTICO E IMPLEMENTACIÓN DE CONTROLES Y MECANISMOS DE SEGURIDAD EN LA RED DE DATOS DE LA ALCALDÍA DE SAN ANTERO CÓRDOBA.

IRINA PADILLA GARCÉS
FRANCISCO JAVIER MOSQUERA ZÚÑIGA

PROYECTO DE GRADO PARA OBTENER TITULO DE ESPECIALISTA EN SEGURIDAD INFORMATICA

DIRECTOR
EDGAR ALONSO BOJACÁ GARAVITO
INGENIERO ELECTRÓNICO

TUTOR
MIGUEL MAHECHA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGIA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAHAGÚN - CORDOBA
2016

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

San Antero Córdoba -

Este es un trabajo que se ha realizado con mucho esfuerzo, dedicación y cariño lo dedicamos a Dios y a nuestras familias que dan todo por nosotros.

AGRADECIMIENTOS

Agradecemos a Dios y a todos los que, con su pequeño aporte en colaboración intelectual, anímica y en trabajo físico han contribuido a la consolidación de este proyecto y a lo que él puede generar si es aplicado en el área donde se desarrollará.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE GRÁFICAS

pág.

ANEXOS

pág.

INTRODUCCIÓN

El crecimiento de las necesidades de TI en la alcaldía de San Antero Córdoba para el mejoramiento de la productividad en los diferentes niveles y áreas ha permitido un crecimiento peligroso, dado a la adición de dispositivos y herramientas para producir con pocas o nulas medidas de seguridad tenidas en consideración al momento de hacer cambios en las estructuras. Con el objetivo de determinar el grado de mecanismos y controles necesarios para tener una plataforma TI controlada se pretende desarrollar este proyecto de diagnóstico e implementación de controles y mecanismos de seguridad en la red de datos como propuesta de solución a la seguridad de la red de datos de la Alcaldía de San Antero Córdoba, para que sean implementados y se logre tener un ambiente de trabajo más controlado y consiente de los riesgos que puede enfrentar la entidad en el área de TI.

La Propuesta de solución con el análisis respectivo de acuerdo a los datos recolectados en las pruebas, monitoreos que se realizarán a la red de datos y las alternativas de solución planteadas mediante esquemas de seguridad definidos y apoyados en los productos del mercado con costo de implementación que se dejará a disposición del administrador del gasto, quién debe evaluar y definir si implementa la solución propuesta para mejorar una situación de necesidad de seguridad detectada en la red de datos de la Alcaldía de San Antero Córdoba.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La revisión y análisis del material encontrado referente al tema a desarrollar en el proyecto se ha podido notar que a nivel de publicaciones educativas e informativas son muy pocos los antecedentes que se pueden hallar relacionado con el tema, el un desarrollo encontrado es realizado por unos estudiantes de la Universidad de las Ciencias Informáticas de La Habana Cuba, con el nombre Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática, según Michel Miranda Cairo, Osmany Valdés Puga, Iván Pérez Mallea, Renier Portelles Cobas , Raúl Sánchez Zequeira [2016], el cual consiste en la creación de una metodología basada en la integración de varios modelos, normas, herramientas y buenas prácticas para la implementación de la gestión automatizada de controles de seguridad informática, la cual combina varios métodos que están orientados a la gestión de riesgos y la enfocan hacia la automatización de las etapas de operación, monitorización y revisión del SGSI (Sistema de Gestión de Seguridad de la Información).

Así mismo se encontró un trabajo realizado en la Universidad Tecnológica de Bolívar, por Martínez Molina Kelly Johanna Y Pacheco Meneses Javys Y Zúñiga Silgado Isaac, (2009). Con el nombre “Firewall – Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y Medianas Empresas)”, con el cual se quiere dar solución a los problemas de seguridad de una red a bajo costo, el cual fue orientado para las pymes, de tal manera que les permitiera identificar y enfrentar con adecuadamente los riesgos y disponer de una solución integral. Para lograr esto, trabajaron en la detección de las necesidades de las PYMES e implementaron un Servidor Firewall Linux. Donde se configuraba un host con la herramienta Iptables quien definía las reglas de filtrado de paquetes de acuerdo a las políticas de seguridad que se establezcan para proteger y controlar el flujo de datos entre dos redes. Ellos hicieron un análisis de la funcionalidad del firewall, instalaron

servicios a los hosts de las redes locales para así poder hacer una revisión de la veracidad y factibilidad de las reglas establecidas, y así descubrieron que el firewall se comportó de manera efectiva y respondió adecuadamente a las exigencias esperadas con las políticas de seguridad creadas.

También se puede referenciar el trabajo desarrollado por los estudiantes David A. Franco, Jorge L. Perea y Plinio Puello de la universidad de Cartagena, quienes tienen como objetivo principal diseñar una metodología para la detección de vulnerabilidades en redes de datos (2012), Un trabajo muy similar al proyecto que se quiere desarrollar, el trabajo en referencia desarrolló una serie de fases que denominó reconocimiento, escaneo de puertos, enumeración de servicios y escaneo de vulnerabilidades, cada una de ellas fue soportada con herramientas de software. Y así obtuvieron resultados que arrojaron una serie de datos que usaron como insumo para la ejecución de las etapas subsiguientes. Para validar la funcionalidad de la metodología que estaban proponiendo usaron la red de datos de la Universidad de Cartagena, en la cual hallaron muchos tipos de vulnerabilidades. Con estos resultados obtenidos determinaron que la metodología propuesta es muy útil para descubrir vulnerabilidades en las redes de datos, lo que le da a este material para el área de la seguridad informática y convierte al mismo en elemento base para la documentación de este proyecto.

La red de datos, vista como el desarrollo más importante y evolutivo en el campo de las comunicaciones, es por tanto una herramienta primordial en toda entidad, siendo así, trabajaremos, en la red de datos de la Alcaldía de San Antero Córdoba como uno de los elementos bases representativos para el desempeño y alcance de objetivos de la entidad, por tal razón este proyecto se ha enfocado en uno de los aspectos a atender, como lo es, la seguridad en la misma, la cual consiste en el trabajo referente a salvaguardar aspectos como seguridad de datos y la protección contra exposición accidental o intencional de los mismos, acceso a red, a los sistemas de información, a la información en tránsito, mediante mecanismos y

políticas de seguridad, por ello tendremos en cuenta conceptos relevantes a cerca del control y la contención de amenazas en la red de datos que muestran a estos como una causalidad de grandes pérdidas en diferentes ámbitos, como lo confirma Cisco en el documento Soluciones de control y contención de amenazas (2007), donde afirman:

Que las amenazas a la seguridad de la red pueden perjudicar considerablemente la productividad e interrumpir actividades y operaciones comerciales, ocasionando la pérdida de información, y en consecuencia provocar pérdidas económicas que desencadenarían sucesos como: el incumplimiento de obligaciones legales. Así mismo está comprobado que la piratería informática continúa trabajando y creando nuevas técnicas para acceder a la información, con fines económicos, con técnicas cada vez más difíciles de detectar. Es por ello que las empresas necesitan soluciones completas, fáciles de administrar y utilizar para afrontar las amenazas de manera anticipada.

Es importante entonces dar especial importancia por parte de la entidad a aspectos de seguridad que permitan resolver una variedad de problemas en este campo, en áreas o aspectos, que según la fuente experta, CISCO son: “la productividad de los empleados y TI en casos de ataques de virus o gusanos, la seguridad de la información confidencial, la protección de la reputación y marca de la empresa, la interrupción en las comunicaciones e impacto en las actividades empresariales cotidianas”.

Otra teoría que sustenta la necesidad de apuntar en el trabajo de la implementación de seguridad en la Alcaldía de San Antero Córdoba y en especial en afrontar los ataques o amenazas de manera más eficaz es la división de seguridad de EMC^2 RSA, Informe Técnico. (2014), la cual han emitido un concepto acerca de que las empresas deben trabajar en: “Detección y respuesta ante amenazas basadas en inteligencia” este concepto es emitido por la empresa en mención que se dedica a

la criptografía y al software de seguridad, por ello la importancia de tener en cuenta las recomendaciones y hacer visible la siguiente sugerencia que se hace sobre cómo las organizaciones deben enfrentar las intrusiones o infiltraciones a la que pueden verse sometidas, de esta manera apuntan a que la seguridad deben apartarse de los métodos pasivos de detección de amenazas y encontrar intrusos de forma activa, por medio de una evaluación constante del ambiente de TI y así ver señales sutiles de cualquier actividad sospechosa o maliciosa a través del desarrollo de capacidades de análisis de datos y de respuesta a eventos, y afirman, lo cual es difícil pero no imposible y debe ser resuelto a pesar de las diferentes limitaciones, según ello, esto se logra solo con la aplicación de seguridad basada en Inteligencia, y para lograrlo se deben realizar las siguientes acciones, para una detección y repuesta eficaz, como lo plantean a continuación:

- ✓ Procurar mantener visible la actividad digital dentro de los logs, la red y las terminales.
- ✓ Usar inteligencia analítica partiendo de los diversos orígenes de datos para revelar amenazas ocultas y a partir de ellas optimizar las decisiones hacia una respuesta eficaz y concreta.
- ✓ Hacer uso de detección de malware sin firmas en las redes y las terminales.
- ✓ Dar un uso eficiente a los equipos destinados a la seguridad, mediante la definición de procesos eficaces, la automatización del flujo de trabajo realiza inteligencia de amenaza y la educación del equipo de seguridad.

As í mismo debe desarrollar capacidades amplias en:

- ✓ Realizar monitoreo permanente e integral a la red y las terminales, por ej.: hacer seguimiento y análisis al comportamiento de los hots.
- ✓ Aplicar la inteligencia analítica, con el fin de tomar todos los datos e información capturada y realizar un análisis descriptivo, predictivo o de

optimización e identificar conductas sospechosas que muestren una ruta a seguir y apresuren la indagación.

- ✓ Hacer análisis de malware sin tener en cuenta firmas de archivos si no, solo el comportamiento de los ejecutables de los datos que se obtienen en las redes y las terminales y así detectar actividades dañinas.
- ✓ Tener practicidad en la detección de incidentes y respuesta a ellos de tal forma que sean agiles el equipo de seguridad y sea acelerado el flujo de procesos y las tareas rutinarias quiten menos tiempo y se posea más tiempo para dedicar a defender las prioridades altas y a solucionar las amenazas más riesgosas.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo definir los controles, mecanismos o políticas adecuados, para integrar seguridad al esquema actual de la red de datos de la alcaldía de San Antero?

1.3 DESCRIPCIÓN DEL PROBLEMA

La Alcaldía de San Antero Córdoba es una entidad pública, que tiene como objetivo principal servir a la comunidad sananterana y a cualquier otra entidad u organización que requiera los servicios que se brindan, en esta misma medida, para tratar de cubrir y cumplir estos objetivos la entidad ha tratado de evolucionar generándose la necesidad de crecer en infraestructura física y tecnológica.

En este camino hacia el crecimiento y adaptación tecnológica, se han desarrollado trabajos que no han sido adecuadamente definidos, esto ha generado carencias en las implementaciones, las cuales dejan vulnerabilidades en la entidad. Debido al desarrollo de proyectos tecnológicos sin esquemas bien diseñados y sin mecanismos y políticas de manejo y uso de buenas prácticas de TI, todas estas carencias tienen expuesta a la entidad a amenazas como:

- ✓ Ataques de por virus o software malicioso a los sistemas críticos y equipos de cómputo en puestos de trabajo
- ✓ Perdida de datos en sistemas críticos y en áreas de oficinas.
- ✓ Perdida de información de la entidad por rotación o salida de personal durante el periodo de gobierno o dentro de él.
- ✓ Mal manejo de los equipos de cómputo y programas u aplicaciones en la red, por parte de los usuarios internos.
- ✓ Accesos no autorizados a los sistemas de información o las herramientas de TI por actores interno o externos.

Los riesgos a que está expuesta la entidad en materia de seguridad informática son variados y en todos los aspectos, la alcaldía carece de mecanismos y políticas de seguridad para la protección de los sistemas, herramientas de TI y para la aplicación de buenas prácticas de TI. Por su crecimiento poco planeado y no esquematizado u orientado hacia un ambiente seguro, ha implementado un sistema de red cableado inseguro, sin dispositivos que monitoreen o hagan control del tráfico o sirvan de escudo en la red de datos, situación que ubica a la red de datos en posición vulnerable, en cuanto al grado de seguridad que debe manejarse para garantizar los principios de confidencialidad, disponibilidad, e integridad de la información que circula, y se mantiene en la misma, para el desarrollo de los procesos en la Alcaldía de San Antero Córdoba, Todo esto la vuelve un elemento deseable y de fácil penetración por cualquiera de los actores internos, externos sean ajenos o no a la entidad, y a los procesos y procedimientos que se desarrollan diariamente por medio de la red de datos. De manera tal que puede la entidad quedar en situación de calamidad o desastre ante la ocurrencia de un ataque al sistema de red y cualquier elemento que pertenezca a ella, porque son muchas las puertas de entrada a los sistemas de la entidad, dado la carencia de controles y mecanismos de seguridad establecidos hoy día.

2 JUSTIFICACIÓN

Dada la Problemática de seguridad que en la actualidad presenta la entidad en su red de datos, es necesario el diagnóstico y la evaluación de la misma, porque solo así, se conocerá la situación de riesgo real que se tiene. Y ello permitirá crear una base de vulnerabilidades a través de las cuales se realizará un análisis y se establecerán puntos guías necesarios a la hora de recomendar controles y medidas que puedan ser aplicadas para mejorar el estado actual de seguridad en la red de datos de la Alcaldía de San Antero Córdoba, de forma tal que se convierta en una red más segura y fortalecida.

Solo a través de la realización de monitoreo, escucha de puertos, dispositivo y equipos en la red, se explotaran las vulnerabilidades y se obtendrán datos cuantitativos de la actividad que se da en la misma, hecho que permitirá plantear soluciones a la situación presente, de manera que se podrán identificar y tratar adecuadamente los riegos y se establecerán controles y mecanismos de seguridad para que la entidad se proteja y alcance logros significativos en este aspecto, cuando implemente las soluciones propuestas.

Para alcanzar todo esto se realizará una investigación a cerca de técnicas, métodos o herramientas disponibles para diagnóstico y para implementación de seguridad Informática, que permitan identificar, definir, acertadamente los controles y mecanismos de seguridad necesarios y adecuados para contrarrestar las vulnerabilidades, de manera que mejore el estado actual de seguridad en la red de datos de la Alcaldía de San Antero Córdoba, y se convierta en una red más controlada. Y así generar como resultado una propuesta de solución de seguridad a la situación, la cual será implementada por la entidad cuando ella defina y establezca los tiempos y el presupuesto necesario para ello.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diagnosticar la seguridad de la red de datos y evaluar los controles y mecanismos a implementar en la alcaldía de San Antero.

3.2 OBJETIVOS ESPECÍFICOS

Levantar información conceptual y estado de arte, métodos, herramientas de diagnóstico de red y controles de seguridad para la red de datos de la alcaldía de san antero.

Realizar el diagnóstico del estado actual de seguridad a la red de datos de la Alcaldía de San Antero.

Diseñar una propuesta de solución de seguridad a la red de datos, documentación y resultados del proyecto.

4 MARCO REFERENCIAL

4.1 ESTADO DEL ARTE

Cuando se iniciaron las comunicaciones el hombre busco formas de hacer llegar mensajes a través de largas distancias como, por ejemplo, señales de humo. Sin embargo, siempre estuvo el inconveniente de mantener segura la información que solo unos pocos podrían manejar.

En la segunda guerra mundial se evidenció muy bien la importancia de mantener una comunicación protegida debido a que los aliados (el grupo de gobiernos que estaban en contra de la Alemania Nazi) encontraron como vulnerar al ejército NAZI al interceptar sus comunicaciones y descifrar las comunicaciones encriptadas. Por este hecho los aliados tomaron ventaja y ganaron la guerra.

A día de hoy el hombre ha ido un paso más alla desarrollando sistemas de comunicación por medios guiados y no guiados permitiendo el desarrollo de nuevas formas de comunicarnos, de comercializar productos, y un sinfín de actividades que implican el manejo de nuestra información personal.

Por estas redes circulan estas y mucha más información que no solo implica a personas, también relacionada con pequeñas empresas, grandes o inclusive países que necesitan resguardar sus datos sensibles, lo cual nos muestra la gran necesidad de tomar medidas. Una muestra de eso son noticias como las de WikiLeaks en las que información sensible de países poderosos salió a la luz generando una serie de malestares en el mapa político. También están esos casos no menos importantes en los que hacen alusión a personas que les vaciaron sus cuentas por internet o artistas que sus fotos íntimas fueron robadas y hoy siguen circulando por la red.

Ahora podríamos seguir mencionando casos como estos, pero vamos más allá, pensemos en las personas que sus vidas cambiaron por completo por una conversación personal que se hizo pública, o por una foto o por perder sus recursos económicos por una mala operación financiera en la red, llevando inclusive a que algunos pierdan hasta sus vidas.

Esto nos muestra que el proteger las redes de datos debe ser tan obvio como colocarle una puerta a nuestra casa y de allí la necesidad que, aunque sean conocimientos básicos todos debemos tomar medidas para protegernos en las redes de datos que utilizamos sea en nuestra casa, cuando estamos en el trabajo o en cualquier otro lugar donde tengamos acceso a internet.

(ROMERO) Nos define un sistema informático como el conjunto de elementos hardware, software, datos y personas que permiten el almacenamiento, procesamiento y transmisión de información.

Estos, los sistemas informáticos, son los que estamos obligados a darle protección teniendo presente criterios de seguridad informática en el que se espera que la alcaldía de San Antero Córdoba pueda cumplir con esos criterios de seguridad, lo cual hace necesario un análisis de su sistema de seguridad y encontrar que tanta vulnerabilidad tienen los sistemas informáticos.

En su “Manual de Seguridad en Redes” (ARCERT, 2013) nos menciona que el aumento de los ataques informáticos es una problemática que va más allá de la idea de que un sistema de informático es seguro porque maneja cuentas de usuarios con algún tipo de seguridad. Las empresas no dimensionan la importancia de la seguridad informática y no implementan medidas de seguridad en sus redes de datos lo cual los convierten en blancos fáciles para los hackers informáticos.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo lo cual es aprovechado por los delincuentes que encuentran en la falta de control y monitoreo de las redes de datos su mejor aliado para realizar acciones poco respetuosas a la privacidad y de la propiedad de recursos y sistemas.

(Bustamante) En su monografía nos menciona las amenazas a la que una red de computadores es susceptible, en la que se destaca en el caso de las amenazas humanas las que son maliciosas (externas e internas) y las no maliciosas que surgen de la ignorancia del personal de la empresa. También menciona las amenazas por parte de los desastres naturales en los que se incluye incendios, inundaciones, terremotos o cualquier otra actividad natural.

Por esto nos menciona 2 tipos de seguridad para estos dos tipos de amenazas, una física y otra lógica. La primera la define como la aplicación de barreras físicas y procedimiento de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Y la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo.

Por esto el SearchDataCenter (Cobb) recomienda implementar los siguientes controles de seguridad para evitar la filtración de datos

Las contraseñas seguras: Aunque se habla mucho del tema, el uso de contraseñas débiles todavía es lo habitual entre personas que buscando recordar de manera rápida las contraseñas de acceso. Inicialmente se buscan contraseñas por defecto que aún no se han cambiado o nombres de usuario comunes con sus respectivas contraseñas.

Cifrado de datos: El cifrado de datos aumenta de manera considerable la seguridad informática debido a que evita problemas relacionados con la pérdida datos. Se puede llevar a cabo mediante el uso de certificados digitales, SSL o IPSec, manteniendo oculta la información sensible de una organización.

Seguridad de los empleados: Uno de los ataques más efectivos a usuarios es el pishing el cual consiste en la suplantación de la identidad de una página WEB. Cuando se capacita al personal con respeto de cuáles son las últimas tendencias de esta modalidad se reduce de forma considerable una amenaza la red.

Filtros de firewall egreso: Los firewalls no solo deben ser usados para controlar el tráfico en la red. Importante que sea monitoreado el tráfico de salida de esta forma evitamos el malware que envía datos a nuestro controlador.

Asegure los servicios de terceros: Cuando se encarga de ciertos aspectos a terceros de la seguridad de la organización puede que estos dejen los espacios que aprovechen los atacantes, por esto es vital saber quién hace la configuración sobre un equipo que un tercero suministra

4.2 MARCO CONCEPTUAL

Otros conceptos bases para tener en cuenta, es mirar la seguridad como una parte funcional importante que complementa la gestión de red, que consiste en hacer una planificación, organización, supervisión y control de elementos de comunicaciones y recursos humanos, para garantizar un nivel de servicio adecuado, de acuerdo con un costo, entonces se toma como referencia estas teorías como base de esta propuesta y se tienen en cuenta conceptos como:

La Seguridad Informática: Parte de la informática que se encarga de velar por la protección de la infraestructura de TI, en especial, la información almacenada y que circula. Mediante la aplicación de estándares, protocolos, métodos, reglas, herramientas y leyes definidas en pro de minimizar los riesgos en infraestructura y en la información, apoyados en este concepto, trataremos de identificar y adaptar las mejores prácticas para generar la propuesta de solución a la necesidad que sea diagnosticada.

Seguridad en redes: concepto que busca garantizar que los elementos y dispositivos de una red de datos trabajen y funcionen de manera óptima, de acuerdo a los permisos que le sean asignados, en cuanto a los principios de disponibilidad, confidencialidad, integridad y trazabilidad, los cuales se deben proteger como garantía de seguridad en una red.

Confidencialidad: Es un principio de seguridad de la información, que permite garantizar que solo quienes sean autorizados para acceder a los procesos y sistemas informáticos son los que deben tener acceso, permitiendo que un actor externo ajeno a un sistema u organización no lea, copie o modifique la información almacenada o circulante en el sistema.

Servicio de confidencialidad de contenido: Tipo de confidencialidad que consiste en proteger el contenido de un recurso del sistema, esto se logra cifrando los paquetes de datos de manera que, al ser capturada por actores externos, no puede ser interpretada, o utilizada la información, sin autorización.

Servicio de confidencialidad del mensaje: Este tipo de confidencialidad consiste en proteger el mensaje durante el proceso de transmisión por el canal o medio, se logra a través del cifrado, por medio de un encapsulamiento que blinda a los paquetes para que no puedan ser descifrado y no se descubran información acerca

del remitente o receptor del mensaje o la frecuencia de envío, en caso de ser interceptados.

Autenticación: Servicio que busca revisar la identidad de quien intente acceder a un sistema informático, de manera que se compruebe que sean quien dicen ser, y se garantice la no suplantación, al momento de realizar una acción o solicitud de un servicio.

Integridad: Principio de la seguridad de la información y servicio que garantiza la veracidad y el valor del contenido o datos en un sistema informático, manteniéndolos inalterados y en orden lógico durante un proceso de comunicación o prestación de un servicio.

Servicio de integridad del contenido: Garantiza que el contenido del mensaje no ha sido alterado.

Servicio de integridad de la secuencia del mensaje: Garantiza que el orden y secuencia lógica del mensaje no fue cambiada durante el proceso de comunicación o prestación de un servicio.

No Repudio: Este servicio garantiza la trazabilidad de la conexión, permitiendo conocer el origen y el destino de transmisión.

No repudio de origen: Garantiza al emisor del mensaje.

No repudio de envío: Garantiza el envío del mensaje.

No repudio de presentación: Garantiza que los datos fueron presentados para el envío.

No repudio de transporte: Garantiza el transporte de los datos, no hay forma de negarlo.

No repudio de recepción: Garantiza la recepción del mensaje.

Control De Acceso: Este servicio se utiliza con el fin de restringir el acceso a las bases de datos que almacenan la información. Y va de la mano con el servicio de autenticación ya que cualquier actor que quisiese acceder a algún recurso del sistema primero deberá identificarse para que sea permitida la entrada a dicho sistema o información según los permisos y privilegios asignados.

Disponibilidad: Principio de la seguridad de la información y servicio que garantiza que los actores autorizados según los perfiles tengan acceso a la información en el momento en que se requiera y las veces que lo soliciten.

Mecanismos de seguridad: son el conjunto de elementos o procesos que se implementan para garantizar control en un servicio o sistema.

Aplicando criptografía a los mecanismos de seguridad, se obtiene control en las comunicaciones, por esta razón es bueno manejar algunos conceptos como:

Código de detección de modificación: Proceso mediante el cual con una suma aplicada a los datos que se transmiten el receptor puede verificar la integridad del paquete recibido, al comprobar mediante una función de comprobación que el paquete arrojó la misma suma aplicada al paquete recibido. En este caso el receptor también recibe la suma.

Código de autenticación del mensaje: En este caso sólo el resultado de la suma está cifrado y solo al momento de que el receptor realiza la prueba de comprobación

se tendrá la certeza que los datos están íntegros y que el emisor es quien se presume los envió.

Firma digital: Una firma digital es una pieza de información que sufre una transformación y a través de una función relaciona de forma única al documento con la clave privada del firmante, por ello se puede decir que las firmas digitales dependen del mensaje y de quien la genera, con el fin de que la información no sea modificada y al mismo tiempo sirve para proporcionar servicios de no repudio ya que el destinatario tendrá la certeza de que el mensaje fue enviado por quien esperaba.

Número de secuencia del mensaje: Cuando un mensaje se divide en varios paquetes para ser transmitido; a cada paquete se le agrega un número el cual puede ir cifrado o no, dicho número es en realidad una secuencia de bits que identifica el número de secuencia del paquete; de esta manera el receptor tiene que comprobar que dicha secuencia de bits corresponde con el número de paquete que está recibiendo. Con este procedimiento se verifica si algún paquete fue insertado o sustraído por un tercer agente durante la transmisión.

Cifrado: Este es un mecanismo que busca que actores o procesos que no tengan autorización les sea difícil leer la información, gracias a métodos de cifrado que la transforman. De esta forma se protege la confidencialidad de los datos, aunque este No es de uso exclusivo para este servicio ya que es usado con otros mecanismos para dar soporte a otros servicios.

Control de acceso: Consiste en el uso de contraseñas para dar autorización de acceso a la información a los usuarios legítimamente autorizados.

Relleno de tráfico: Consiste en la transmisión y envío de datos falsos de la misma forma que se transmite la información legitima, de tal forma que si se está ejecutando un análisis de tráfico no se conozca si realmente la información es correcta y útil.

Control de encaminamiento: Consiste tener la opción de en enviar la información por una ruta alterna cuando se detecta un ataque a la conexión.

Certificación: Consiste en emitir una certificación por un tercer actor de confianza, y este garantiza la integridad, secuencia y frecuencia de los datos, de lo cual deben dar fe el emisor y receptor de los datos.

También se tomará como base teórica para tener en cuenta, lo expresado en cuanto a los siguientes mecanismos, según la misma publicación:

Mecanismos de Seguridad Generalizados de OSI: Son mecanismos utilizados para agregar mayor seguridad en la comunicación entre dos entes y de acuerdo con el nivel requerido será su uso. La arquitectura de seguridad OSI se define cinco mecanismos, de la siguiente manera:

Funcionalidad de confianza: Este tiene que ver con todos los procedimientos a desarrollar para dar seguridad a la comunicación y ver que realmente se cumpla con el objetivo como se previó.

Etiquetas de seguridad: Consiste en etiquetar los recursos del sistema de forma que se identifique la clase de información por niveles de seguridad: secreta, confidencial, no clasificada, entre otras, con el fin de identificar la sensibilidad o nivel de protección que se requiere para cada recurso identificado.

Detección de eventos: Este mecanismo se usa para detectar violaciones aparentes de la seguridad. Donde se podrán percibir todo tipo de eventos ocurridos en el sistema, como violaciones o accesos legítimos.

Rastreo de auditoría de seguridad: Consiste en la realización de una verificación de los registros y actividades del sistema para validar si se cumplen las políticas de seguridad definidas y así brindar eficientemente seguridad al sistema; en caso de fallas se realizan recomendaciones y se hacen los cambios para solucionar los problemas.

Recuperación de seguridad: Este mecanismo permite recuperar el sistema en caso de alguna falla, de acuerdo a las medidas definidas previamente y resultantes de una serie de pruebas verificables de acuerdo a criterios y normas.

En esta misma medida podemos encontrar el otro aspecto a manejar son los ataques, que pueden ser variados y de diferentes tipos:

Identificando un ataque como infracción a la seguridad y que es realizado por intrusos que accede al sistema violando las restricciones, con el objetivo robar, manipular, causar daño en el sistema de información o provocar pérdida de valor.

Según publicación de la Universidad autónoma de México, Existen dos tipos de ataques:

Pasivo, en este el intruso sólo busca obtener información y sin modificarla, en estos casos resulta difícil saber que se es atacado.

Activo, aquí el intruso entra para obtener la información y la modifica para sus intereses, lo cual si permite darse cuenta que se está sufriendo un ataque.

Los ataques se llevan a cabo por medio de etapas, donde el intruso va alcanzando metas en su intensión de penetrar un sistema de información, dispositivo informático, o red. Y se pueden presentar por la existencia de vulnerabilidades el diseño, configuración y operación de los sistemas, lo que en ocasiones provoca desastres en las organizaciones y puede causar grandes pérdidas.

Las vulnerabilidades a nivel de las organizaciones han venido cambiando de acuerdo con la evolución en la tecnología y al perfeccionamiento de las técnicas de los intrusos, entre las formas de encontrar vulnerabilidades están:

La Ingeniería Social, es una táctica que se usa para a través de un usuario con autorización, sacar información relevante del sistema, sea por medio de engaños o solicitudes falsas, fingiendo ser oficiales de compañeros de trabajo y se aprovechan del desconocimiento o ignorancia del usuario legítimo.

Factor Insiders, este tipo de vulnerabilidad es explotada por personal interno de la organización, se porque entró y se ganó la confianza y utiliza esos privilegios para atacar y sacar información o por causas de descontento y disgusto y genera una reacción buscando venganza.

Códigos Maliciosos, estos consisten en la utilización de programas o aplicaciones maliciosas (malwares) que buscan hacer daño en los sistemas informáticos, los más comúnmente usados son virus informáticos, troyanos, Back doors, keyloggers, gusanos, spyware, rootkits, entre otros.

Contraseñas: consiste en buscar la manera de acceder a las contraseñas de los sistemas de información y aplicaciones, algunas veces es posible por la debilidad de las mismas o porque quedan a la vista de otros, o se obtienen por medio de

tácticas como fuerza bruta, uso y acceso a diccionarios, además de estos, también se pueden aprovechar de errores como:

Utilizar la misma contraseña en varias en todas las cuentas y servicios.

Acceder desde lugares públicos a servicios que utilizan autenticación, corriendo el riesgo que los atacantes pudiesen haber infiltrado programas que capturen la información o dispositivos físicos como keyloggers.

Usar protocolos de comunicación inseguros, como el correo electrónico, navegación web, chat, que transmiten información en texto sin cifrar.

Técnicas como shoulder surfing (mirar por encima del hombro), que permiten evadir los controles programados de seguridad, las cuales se hacen de manera directa, espionaje.

Configuraciones Predeterminadas o por defecto: La configuración predeterminada está definida por los parámetros que los sistemas operativos y las aplicaciones y cualquier desarrollo tiene determinado como valor por inicial o mínimo o requerido para el lleno de requisitos para funcionar sin errores, no implicando que sea la mejor configuración y seguridad aplicada. Y partiendo de que son conocidos en su mayoría por ser parámetros estándares conocidos.

Así mismo, la intromisión ha sido identificada por fases de ejecución, según publicación, como:

El reconocimiento, donde se estudia a la víctima potencial, aplicando técnicas que ayudan al logro del objetivo.

La exploración: en este momento ya se tiene captura de datos recolectados en la fase de reconocimiento y se procede a analizarlos para identificar su importancia y valor como determinar si son contraseñas, direcciones IP, etc.

Conseguir el acceso: es la fase donde se analizan las vulnerabilidades encontradas y se inicia las técnicas de ataque.

Mantener el acceso: esta es la fase del proceso del ataque, en el cual ya estando dentro de sistema atacado, se pretende tener la facilidad de entrar cuando se requiera, como un usuario más, esto lo logran usando back door, gusanos, etc.

Borrado de huellas: en algunos casos dependiendo la intencionalidad del ataque, el intruso intenta eliminar todo rastro que haya podido dejar y mostrar la actividad realizada por él.

Los sistemas cifrados también son enfrentados a ataques activos, y se dividen en dos tipos: Ataques a los métodos de cifrado, Ataques a los protocolos criptográficos

Ataques a los Métodos de Cifrado: Este ataque busca obtener la clave secreta para descifrar cualquier criptograma, esto se logra sacando provecho a las vulnerabilidades que pueda tener el método de cifrado.

Ataque sólo con texto cifrado: Este se ejecuta porque el criptoanalista posee el criptograma, el algoritmo que lo generó y con esta información trata de conseguir el texto legible del mensaje.

Ataque con texto original conocido: Se presenta cuando el criptoanalista conoce el mensaje legible, el criptograma y el algoritmo que lo generó; con estos datos se busca conseguir la clave secreta y poder desencriptar cualquier tipo de texto.

Ataque con texto cifrado escogido: Para ejecutar esto el criptoanalista debe contar con el algoritmo de cifrado, elegir un criptograma y también poseer un texto legible del mismo, con ello busca obtener el mensaje legible de cualquier criptograma que recepcione.

Ataque con texto escogido: Para este tipo de ataque el criptoanalista usa el algoritmo de cifrado y el criptograma que quiere descriptar, y el criptograma de un texto legible que él escoja más otro texto legible de un criptograma también seleccionado por él.

Ataques a los Protocolos Criptográficos: Este ataque no consiste en descubrir claves secretas para conocer los mensajes, sino que trata de encontrar la manera de encontrar información para vulnerar los protocolos criptográficos, de manera que se rompan las medidas de seguridad establecidas y los objetivos trazados por las entidades para establecer la comunicación. A continuación, tenemos una serie de ejemplos:

Ataque con clave conocida: Aquí se procede a trabajar con claves usadas en cifrados anteriores y así intentar conocer claves nuevas.

Suplantación de personalidad: Aquí se saca provecho de autorizaciones legítimas y obtienen sin ningún problema los mensajes legibles.

Compilación de un diccionario: Se saca provecho de las bases de datos que contienen la información cifrada de autenticación de usuarios legítimos y si se usa cifrado público, el intruso puede usar claves aleatorias y luego las cifra para así encontrar alguna en el diccionario. Y si esta llega a coincidir, tiene una forma de acceder al sistema con la clave encontrada.

Búsqueda exhaustiva: Para realizar esta clase de ataque se genera aleatoriamente todos los valores posibles de claves de acceso y se prueban hasta encontrar la coincidente y valida.

Ataque de hombre en medio: Consiste en ubicarse en medio de la línea de comunicación entre dos actores autorizados y se captura la información de uno de ellos y se le envía al otro luego de haberla recepcionado y leído.
En este mismo orden se encuentran los ataques a las redes, que aprovechan las vulnerabilidades de las capas del modelo de red, en este caso se enumeran los asociados al modelo OSI y TCP/IP [10]:

DNS Spoofing, se da al momento de que se solicita conexión a un servicio y es necesario traducir un nombre de dominio, aquí el atacante cambia la información por una falsa, sea un IP o un nombre.

Sniffing, denominado también olfateador, consiste en capturar toda la información y tráfico que pasa sin cifrar por el medio, lo configuran en modo promiscuo de forma que almacena en un log todo el tráfico que pasa por la tarjeta de red, sea generado por mismo sistema o desde/hacia otros sistemas en el entorno compartido, para evitar sea descubierto trabaja en conjunto con troyanos modificados.

Eavesdropping, es una variación del sniffing que almacena la información que captura del computador del atacante (descarga), no solo del tráfico de red.

SMTP Spoofing y Spamming, consiste en cambiar la dirección de origen de un correo electrónico, y se envía el mensaje a nombre de otra fuente, dado que no hay mecanismo de autenticación cuando se establece la conexión TCP al puerto asociado.

DoS (Dnial of Service attacks), denegación del servicio, consiste en exceder los recursos disponibles y definidos para un servicio específico, consiguiendo la caída temporal del servicio, ej. Un servicio que atienda 10 clientes por segundo y reciba 50 peticiones de servicio, entonces parte del tráfico legitimo recibirá como respuesta una negación o hasta se produzca un silencio total para todos, es decir, no tengan respuesta.
Generalmente los ataques DNS son específicos, a servidores, routers, enlaces, con ellos no sufre daño la información, solo busca obstaculizar el acceso al servicio de parte de los usuarios que lo solicitan.

Smtp Flood, consiste en envío masivo de correos electrónicos a listas de usuario de manera continuada, produciendo la recarga de los servidores de correo destino o intermedio.

Buffers- Overflobs, consiste en sobrecargar la capacidad de memoria definida para recibir y manejar datos de las aplicaciones que se ejecutan, en una máquina.

Escaneo de Puertos, con el uso de un programa se analizan el estado de los puertos de un dispositivo o computadora conectada a la red de datos. De forma que verifique si algún puerto está abierto, cerrado, o protegido por un firewall. De manera que se encuentren los servicios comunes ofrecidos y las posibles vulnerabilidades según los puertos abiertos.

TCP SYN Flood, consiste en la solicitud masiva de establecimiento de conexión (SYN) en contra de un sistema, de forma que se reserve una cantidad de memoria en los buffers, en especie de reserva para las nuevas conexiones solicitadas, y se queda esperando la respuesta para el establecimiento de conexión, hasta que se llena de solicitudes falsa, hasta tumbar el servicio, este es una especie de DoS.

Escaneo Basado en el Protocolo ICMP, encontramos:

ICMP Echo, esta es una técnica usada para determinar los equipos activos en la red, generalmente se acede remotamente, con una solicitud ICMP Echo (8) y en espera de una respuesta ECHO Reply (0), de esta forma se sabe si hay actividad en alguna estación.

IP Spoofing, consiste en la generación de paquetes IP, que tiene una dirección falsa, de forma tal que desde la misma maquina se identifique un destino objetivo, debido a que se permite el tráfico de paquetes con la dirección recibida de fuente, y se ha establecido una relación de confianza entre los dos sistemas.

Smurf, Consiste en sacar provecho de una dirección broadcast, cuando el atacante puede enviar un paquete de datos a esa dirección, provocando que todos los sistemas pertenecientes a dicha red respondan simultáneamente.
Cuando se asocia esta técnica con IP Spoofing, al remitir un paquete ICMP con la dirección IP fuente (maquina a objetivo del ataque) y la dirección de destino (dirección broadcast) de una red con un gran número de hots, entonces todas las repuestas (broadcast) serán dirigidas a la dirección IP del sistema “spoofeado”. Este ataque se denomina SMURF.

Routing Protocols, este ataque aprovecha la vulnerabilidad de los protocolos de enrutamiento, de manera tal que cuando se envían la actualización de rutas, se manipula esta y se altera el camino por donde seguirá el tráfico, logrando así el objetivo del atacante.

ARP Spoofing, consiste en infiltrarse en una red Ethernet (basada en Switch y no en Hubs), la cual deja al atacante rastrear paquetes de datos en la red LAN, de forma tal que modifica el tráfico e incluso podría detener el tráfico, mediante el envío de mensajes ARP falsos, con el fin de relacionar la MAC del atacante con la IP de otro nodo (nodo atacado).

Man in The Middle (Sniffing), el atacante se vale de ARP Spoofing, logrando que todos los paquetes que circulan pasen primero por su equipo del atacante.

Denial of Service (DoS) por ARP Spoofing, también se vale del ARP Spoofing, de forma que logra que un equipo crítico de la red tenga una dirección MAC inexistente, consiguiendo que los paquetes dirigidos a dicha IP se pierdan.

Herramientas de Diagnóstico de Seguridad libres o comerciales

Para la realización de un diagnostico en la red de datos es necesario acudir a la utilización de herramientas que manejan un innumerable número de posibilidades para explorar la actividad en le red de datos, algunas se identifican como software libre y no-libres, entre las más usadas están:

Nessus, Esta herramienta es "Open Source" muy reconocida, funciona para Linux y para FreeBSD/NetBSD/OpenBSD y sistemas UNIX no-libres. Permite detectar vulnerabilidades y ofrece soluciones para problemas de seguridad después del escaneo. Es una aplicación pagada que maneja una base de datos con una diversidad de vulnerabilidades definidas, por lo cual ella permite determinar cuáles de esas debilidades se encuentran existiendo en el sistema monitoreado. Y permite parametrizarlo para hacer un trabajo definido y delimitado.

Ethereal o Wireshark, este es analizador de protocolos en la red, funciona en Windows y Linux y es libre, captura los paquetes que circulen por la red, permite saber si se está usando la red para enviar datos hacia otra red, permite ver el flujo reconstruido de una sesión de TCP

Snort, esta herramienta es sniffer (analiza tráfico en tiempo real y registra paquetes en red). Es libre, muy flexible y permite almacenar sus bitácoras en archivos de texto y en bases de datos abiertas como MySQL. Implementa un motor para detección de ataques y barrido de puertos, permite hacer el registro, da alertas y responde

ante anomalías previamente determinadas. Por medio de complementos de terceros puede actuar como un IDS.

Windump, esta herramienta funciona para Windows, es una versión modificada de tcpdump que funciona para Linux, se trabaja por línea de comandos, interceptar y muestra paquetes, TCP/IP o de otro tipo en la red. Para que funcione se debe instalar las librerías de WinPcap.

Netcat, esta herramienta permite depurar diversos problemas en la red, conocida como la navaja suiza, con ella se puede leer y escribir datos en la red mediante los protocolos TCP o UDP. Fue desarrollada para ser una utilidad de tipo "back-end".

Traceroute/Ping/Telnet/Whois, todas esta son herramientas son básicas, permiten hacer auditoria como es: puede conocerse la ruta hasta el destino, permite comprobar si hay conexión a nivel de red, identificar quien es el propietario de un nombre de dominio o de una dirección IP respectivamente.

Fport, esta herramienta se ejecuta en modo comando a través de símbolo de sistema permite ver que puertos fueron abiertos, sean conocidos o no. permite saber qué aplicación abrió los puertos y las aplicaciones asociadas.

Axence NetTools, es una herramienta que busca dar una solución para el diagnóstico que permite detectar todo lo relacionado con las conexiones a la red, tanto para efectuar un simple control, así como para saber si existe alguna irregularidad.
Es una herramienta gratuita para Windows, realiza la detección de dispositivos conectados a la red, tiene editor remoto del registro de Windows y visor del registro de eventos, visor de procesos y de los servicios activos, diagnóstica los servicios TCP y UDP a por medio de conexión de bajo nivel, brinda también la posibilidad de realizar diagnósticos a protocolos no estándares y muestra una visión eficaz de la

información que estuviese disponible a través de SNMP. Incluye NetWatch, WinTools, NetStat, Local info, Network scanner, Service & port scanner, TCP/IP workshop, SNMP Browser entre otras.

Kali Linux, Es una distribución de Linux avanzada, para pruebas de penetración y auditorías de seguridad.

NMAP, Herramienta de software para escanear redes, la cual ayuda a detectar los servicios que se ejecutan en dispositivos remotos, también detecta equipos activos, existencia de filtros o firewalls, sistemas operativos en el equipo remoto, etc.

DVL – DVWA, Damn Vulnerable Linuxy (DVL) y Damn Vulnerable Web Application (DVWA). Aunque el primero está descontinuado, se dice que aún se puede conseguir en Internet para hacer los primeros pasos y primeras pruebas. Es un sistema operativo y una aplicación web que poseen todo tipo de vulnerabilidades, de manera que, al utilizarla, se pueden intentar explotar y experimentar para monitorear el sistema.

4.3 MARCO CONTEXTUAL

En sus inicios la Alcaldía de San Antero Córdoba realizaba sus actividades sin equipos electrónicos y ha ido pasando por diferentes etapas en el tiempo de acuerdo al desarrollo de las decisiones administrativas internas, de acuerdo al administrador de turno y a la capacidad económica del momento en la Alcaldía habían venido introduciendo mejores herramientas de trabajo esporádicamente y remplazando las herramientas manuales, hasta la llegada de los equipos de cómputo a eso del año 1996, cuando inician con el uso de los primeros computadores de escritorio, en el 2000 se introducen también los primeros programas para el manejo y administración en el área presupuestal, de tesorería y de impuestos en la hoy llamada secretaría de Hacienda, desde este momento han realizado inversiones pequeñas en diferentes lapsos de tiempo, para tratar de amoldar a la entidad al desarrollo y uso

de tecnología más actual, en este proceso interconectan los primeros pc´s de escritorio por medio de un Hub, como simple medio de interconexión para trabajar con el software adquirido. Al ir adquiriendo más pc's se cambian a switch y se siguió trabajaron así por varios años, hasta que en 2013 los directivos deciden realizar el proyecto de actualización de hardware e implementan del cableado estructurado, pero sin un análisis previo para una solución integral que involucrara dar y mantener seguridad y quedase plasmada en el diseño para la implementación. De esta forma podemos ver que la necesidad de la Seguridad en la red de datos de la Alcaldía de San Antero Córdoba, nace con el tiempo. En la medida que se va volviendo más activa e interconectada la comunicación y se inicia la utilización de la red de datos como herramienta para facilitación de comunicación y compartición de recursos; este crecimiento de actividades en ella y los diferentes actores que entran a participar como interlocutores en el proceso de intercambio, administración, mantenimiento y almacenamiento de información, requieren mantenerla disponible, segura y con accesos definidos para quienes manejaran informaciones de carácter privado, debido a que pudiera llegar a manos equivocadas y podría usarse con fines dañinos.

Es por todo esto que a medida que se ha crecido, se tiene que ir implementando medios y mecanismos que ayuden a proteger y garantizar la seguridad en la red de datos y cumplir con los reglamentos que exige la ley, en cuanto a proteger la entidad de la ocurrencia de los delitos más frecuentemente denunciados y tipificados por la ley 1273 de 2009, en Colombia. Razón por la cual nace el diagnóstico e implementación de controles y mecanismos de seguridad en la red de datos de la alcaldía de San Antero Córdoba, dado que este es un aspecto muy importante para detectar y subsanar cualquier vulnerabilidad o falla que se tenga en la entidad y que pueda ocasionar riesgos en los procesos y la estabilidad, credibilidad y el respeto y confianza de los usuarios al solicitar o acceder a los servicios.

4.4 MARCO LEGAL

Ley 1273 de 2009[1].

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Que nos dice:

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema

[1] MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LA COMNICACION TIC DE COLOMBIA. Ley 1273 de 2009 de la protección de la información y de los datos. [Consultado 10 de Mayo de 2015]. Disponible en Internet: www.mintic.gov.co/portal/604/articles-3705_documento.pdf

informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

LEY 1341 DE 2009[2]

La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio,

[2] MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMNICACIONES TIC DE COLOMBIA. Ley 1341 de 2009 del marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones. [Consultado 10 de Mayo de 2015]. Disponible en Internet: www.mintic.gov.co/portal/604/articles-3707_documento.pdf

la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.

Que así mismo, la anotada Ley determinó que es función del Estado intervenir en el sector de las TIC con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dicho sector.

LEY ESTATUTARIA 1581 DE 2012[3]

Por la cual se dictan disposiciones generales para la protección de datos personales. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el

[3] MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMNICACIONES TIC DE COLOMBIA. Ley 1581 de 2012 para la protección de datos personales. [Consultado 10 de mayo de 2015]. Disponible en Internet: http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Artículo 2°. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.
El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia.

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales.

e) A las bases de datos y archivos regulados por la Ley 1266 de 2008

f) A las bases de datos y archivos regulados por la Ley 79 de 1993.

Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

Artículo 3°. Definiciones. Para los efectos de la presente ley, se entiende por:

a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

b) Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento;

c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;
d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;

e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;

f) Titular: Persona natural cuyos datos personales sean objeto de Tratamiento;

g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Artículo 4°. Principios para el Tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley.
Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

4.5 RECURSOS

Para el desarrollo de este proyecto es necesario contar con diversos recursos, humanos, técnicos, tecnológicos, y muy posiblemente económicos.
Tabla 1 Recursos económicos

ITEM	DESCRIPCIÓN	DESCRIPCIÓN	Costo
1	Herramientas de Software	Auditoria informática	3.200.000

2	Recurso humano (Técnico, Ingeniero, etc.)	Ing. Sistemas	8.700.000
3	Dispositivos (computadores, router, switches, tarjetas inalámbricas)	Computadores escritorio	7.500.000
4	Elementos de Utilería (papel, tinta, cámaras, etc.)	Resma Papel carta	250.000
5	Recurso Económico	Transporte	$ 350.000
Total			20.000.000

Fuente: Autores

5 DISEÑO METODOLÓGICO

Este trabajo desarrollará un tipo de investigación Descriptiva dado que nos permitirá a través del conocimiento de situaciones y actitudes en el comportamiento de la población objetivo de la investigación describir de manera exacta las actividades, proceso, personas y comportamientos de la red de datos para obtener la caracterización de la realidad en estudio.

Mediante la aplicación de un método deductivo, se inferirá con el análisis de los datos particulares recolectados un concepto general del estado de la seguridad de la red de datos de la alcaldía de San Antero Córdoba, para llegar al producto, el diagnóstico del estado actual a través de los datos cuantificables recogidos con herramientas de monitoreo y auditoria informática, que van a permitir llevar una estadística cuantitativa y cualitativa de las vulnerabilidades y los hallazgos encontrados.

5.1 ALCANCE

Este proyecto busca realizar propuesta de solución de seguridad a la red de datos de la Alcaldía de San Antero Córdoba que quedará documentada y soportada, mediante el desarrollo de un diagnóstico previo, de la situación actual, usando herramientas y técnicas de auditoria informática, como KALI LINUX o NESSUS, las cuales poseen un gran número de sub-herramientas para realizar monitoreo, escucha de puertos, y seguimiento a dispositivo y equipos en la red de datos, de manera que se puedan detectar y explotar vulnerabilidades para obtener datos cuantitativos y cualitativos que permitan realizar un análisis del comportamiento y del tráfico en la red de datos, esto a través de la escogencia de una población objetivo estratégicamente ubicados en cada área de trabajo, con una aplicación de muestreo de un individuo por área de trabajo para obtener datos para luego realizar

una tabulación de eventos encontrados y analizar los mismos para así plantear un esquema de seguridad conformado por mecanismos, políticas y dispositivos necesarios para mejorar la situación de seguridad detectada en la red de datos.

Presentando como producto final una propuesta, documentada y soportada con cada una de las pruebas realizadas y los resultados obtenidos, y soportes de las anomalías encontradas, comparativos, documento monográfico, presupuesto estimado del costo de la solución de seguridad recomendada como mejor opción para implementación de parte de la Alcaldía de San Antero Córdoba. Quedando a disposición de la entidad la implementación de la solución.

5.2 DELIMITACIÓN

Imagen 1 Alcaldía de San Antero

Fuente: Google Maps

Imagen 2 Vista Frontal Palacio Municipal San Antero, Córdoba

Fuente: Google Maps

El desarrollo se realizará a la red de datos, en la El Palacio Municipal “Feliciano Pérez García” Ubicado en la Cra. 14 N° 12D-13 Centro, Bloque Principal de la Alcaldía de San Antero Córdoba, Departamento de Córdoba. El cual está conformado por seis Dependencias, Secretaría de Hacienda, Secretaría de Jurídica y Asuntos Administrativos, Secretaría de Planeación, Secretaria de Salud, Secretaría de obras Públicas, que son cinco áreas directivas y once oficinas del bloque principal del palacio municipal, las cuales se encuentran en una red LAN, interconectadas por medio de cableado estructurado. Cada Dependencia tiene unas áreas de oficinas y un grupo de recurso humano a cargo, el entorno físico está definido por una edificación de cuatro secciones de dos pisos cada uno, que representan 19 áreas de trabajo y un grupo humano de aproximadamente 59 personas con acceso a la red de datos desde su puesto de trabajo. Las cuales están interconectadas por cable cat 6ª. Esta red cuenta con un centro de control o cuarto de cableado, donde reposa los dispositivos que brindad la conectividad, pero no posee ningún nivel de seguridad administrable o configurable en ellos.

5.3 INSTRUMENTOS

El desarrollo de este trabajo estará basado en la realización de pruebas de monitoreo y detección de vulnerabilidades a una muestra diciente de los dispositivos activos de la red de datos y la aplicación de encuestas a una población muestral de personas para validar el cumplimiento y aplicación de las buenas prácticas de Seguridad de la información basadas en la ISO27001:2013.
Lo anterior como herramientas de recolección de datos para la realización del análisis. Mediante una investigación descriptiva y un método deductivo para hacer las tabulaciones y comparaciones de estos.

5.4 PRODUCTO DEL DESARROLLO DEL PROYECTO

Luego de escoger entre la más accesible herramienta para el caso, y realizar una serie de pruebas y monitoreo en la red de datos, se desarrollará un análisis de la situación y se propondrán esquemas o dispositivos necesarios para mejorar la situación de seguridad detectada, generando un documento propuesta de solución de seguridad a la red de datos, como producto final de soporte con cada una de las pruebas realizadas y los resultados obtenidos, se desarrollará un presupuesto aproximado del costo de la solución propuesta. Para dejar a disposición de la entidad el desarrollo e implementación de la misma. La cual deberá implementar para integrar seguridad a su red de datos.

Como producto final se entregará:

Diagnóstico del estado actual de seguridad a la red de datos de la Alcaldía de San Antero. Mediante Informe comparativo del cumplimiento que se está aplicando de la ISO 20071:2013

Documento monográfico del desarrollo del proyecto con información conceptual y estado de arte, métodos, herramientas de diagnóstico de red y controles de seguridad para la red de datos de la alcaldía de san antero.

Propuesta de solución documentada de acuerdo con la situación de seguridad detectada en la entidad basada en las pruebas y resultados del proyecto.

5.4.1 Informe comparativo del cumplimiento entre el sistema actual de la alcaldía municipal de san antero córdoba y el estándar iso27001:2013

Tabla 2 Valoración de los objetivos de control y controles.

OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.5.1 Política de la seguridad de la información.			
A.5.1.1. Están establecidas las políticas para la seguridad de la información, con aprobación por la alta dirección, fue publicada o comunicada a los funcionarios y partes interesadas en la entidad			X
A.5.1.2. La entidad realiza la revisión de las Políticas para Seguridad de la Información en periodos cronogramados o cuando hay cambios importantes, con el fin de garantizar la idoneidad, su ajuste y eficacia continúa de acuerdo a la sinergia.			X
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			

A.6.1.1 La alcaldía establece un marco de referencia para llevar control y operar la seguridad de la información			X
A.6.1.2. La entidad realiza una separación de las tareas y áreas de responsabilidad que chocan, con el fin de reducir la probabilidad de alteración no autorizada o no intencional o el uso inapropiado de los activos de la Alcaldía.			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.6.1.3. Están Definidos y establecidos en la entidad los canales de comunicación con las autoridades pertinentes.			X
A.6.1.4. Están definidos y se mantiene contacto la entidad con grupos de interés especial, comités y profesionales especializados en seguridad informática.			X
A.6.1.5. La entidad cuando maneja proyectos, da manejo a la seguridad de la información de manera independiente al tipo de proyecto que esté planeando o desarrollando.			X
A.6.2. Dispositivos móviles y trabajo remoto			
A.6.2.1 La entidad tiene diseñada y adoptada una política y mecanismos de control que le permita manejar los riesgos generados por el uso de dispositivos móviles.			X
A.6.2.2. La entidad tiene diseñada y adoptada una política y mecanismos de control de			X

seguridad para proteger la información que se maneja mediante teletrabajo			
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS			
A.7.1. La entidad les comunica a los empleados y contratistas sus responsabilidades, de manera que estos las comprendan.		X	
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.7.1.1. La entidad verifica los antecedentes de los candidatos al empleo y lo hace según las leyes, reglamentos, ética y verifica que son idóneos en los roles para los que son considerados.			X
A.7.1.2. La entidad al hacer las vinculaciones a empleados o contratistas incluye en los contratos cláusulas de responsabilidad o confidencialidad en cuanto a seguridad de la información.			X
A.7.2. La entidad se asegura de que los empleados y contratistas crean conciencia de sus responsabilidades de seguridad de la información y que las cumplan.			X
A.7.2.1. La alta dirección en la entidad exige a todos los actores (empleados y contratistas) la aplicación de la seguridad de la información conforme las políticas y procedimientos definidos.			X
A.7.2.2. En la entidad todos sus funcionarios reciben educación y formación para la			X

concientización a cerca de la seguridad de la información, y las políticas y procedimientos asociados a sus cargos.			
A.7.2.3. La entidad cuenta con un proceso definido, establecido y comunicado para el manejo de sanciones cuando se cometen violaciones a la seguridad de la información.			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.7.3. La entidad tiene un proceso definido para proteger los intereses de esta, cuando hay cambio o terminación del empleo.			X
A.7.3.1. La entidad cuenta con un proceso de comunicación definido que permita el cumplimiento de las responsabilidades y los deberes en seguridad de la información luego de la terminación o cambio del empleo y los hace cumplir.			X
A.8. GESTIÓN DE ACTIVOS.			
A.8.1. La entidad tiene identificados los activos y definidas las responsabilidades para una protección adecuada.			X
A.8.1.1. La entidad tiene identificados y asociados los activos relacionados con las instalaciones de procesamiento de información y mantiene un inventario de estos.			
A.8.1.2. Los activos relacionados en el inventario de la entidad son propios.	X		

A.8.1.3. Están identificadas, documentadas e implementadas las normas para el uso aceptado de la información y los activos relacionados en el inventario con las instalaciones de procesamiento			X
A.8.1.4. En la entidad todos los actores (empleados y contratistas) hacen devolución de los activos que tienen a su cargo cuando termina su empleo o contrato.		X	
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.8.2. Clasificación de la Información.			
A.8.2.1. La entidad cuenta con un esquema que permita tener clasificada la información según normas legales, valor, criticidad, privacidad, e integridad de la misma.		X	
A.8.2.2. La entidad cuenta con procedimientos que permitan etiquetar la información según el esquema de clasificación definido para ello.			X
A.8.2.3. La entidad cuenta con procedimientos que permitan dar manejo a la información según el esquema de clasificación definido.			
A.8.3 Manejo de medios de soporte.			
A.8.3. Se Previene la divulgación, la modificación, el retiro o la destrucción de la información en medios de respaldo.			X
A.8.3.1. La entidad cuenta con procedimientos que permitan dar gestión a la información almacenada en medios removibles, según el esquema de clasificación definido.			X

A.8.3.2. La entidad cuenta con un procedimiento que garantice el manejo seguro de los medios de soporte de información removibles cuando ya no se usen de manera formal.			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.8.3.3. La entidad garantiza la protección de los medios que contienen información contra acceso no autorizado o uso indebido durante el transporte		X	
A.9. CONTROL DE ACCESO.			
A.9.1. La entidad tienen procedimientos para controlar el acceso a la información y a las instalaciones de procesamiento de la misma.		X	
A.9.1.1. La entidad tiene definida, documentada y revisada una política de control de acceso, de acuerdo al esquema de clasificación de la información.			X
A.9.1.2. La entidad tienen control de acceso a los usuarios cuando ingresan a la red o a los servidores según perfiles autorizados.			X
A.9.2. Gestión de Acceso de Usuarios.			
A.9.2.1. La entidad cuenta con un proceso de registro y cancelación de los registros de los usuarios para controlar el derecho a acceso.			X

A.9.2.2. La entidad cuenta con un procedimiento definido para el control de acceso formal donde asigne o cancele los derechos de acceso en todos los sistemas y servicios a todos los usuarios.		X	
A.9.2.3. La entidad controla la asignación de derechos de acceso privilegiados en los sistemas y servicios.		X	
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.9.2.4. La entidad maneja un procedimiento de gestión formal para la asignación y autenticación con clave secreta.			X
A.9.2.5. la entidad realiza revisión periódica a los usuarios con derechos de acceso.			X
A.9.2.6. La entidad quieta o ajusta los derechos de acceso a los usuarios de acuerdo a las funciones o al cambio d empleo o contrato.	X		
A.9.3. Responsabilidades de los usuarios.			
A.9.3.1. La entidad exige a los usuarios que apliquen y cumplan las disposiciones de uso de la información de autenticación secreta.		X	
A.9.4. Control de Acceso a Sistemas y Aplicaciones.			
A.9.4.1. La entidad maneja y aplica una política de control de acceso de acuerdo a la criticidad de la información.		X	
A.9.4.2. La entidad maneja un procedimiento de conexión segura como lo determina la			X

política de control de acceso cuando se accede a los sistemas y aplicaciones.			
A.9.4.3. La entidad cuenta con sistemas de gestión de contraseña interactivos que garanticen contraseñas de calidad.			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.9.4.4. La entidad tiene control sobre el uso de programas utilitarios con privilegios que pueden inutilizar el sistema y los controles de las aplicaciones.			X
A.9.4.5. La entidad tiene control sobre el código fuente que puede ser manejado en los equipos.			X
A.10. CRIPTOGRAFÍA			
A.10.1. La entidad se asegura del uso responsable y eficiente de la criptografía para resguardar la confiabilidad, la autenticidad y la integridad de la información.			X
A.10.1.1. La entidad tienen definida e implementada una política que permita usar la criptografía para la protección de la información.			X
A.10.1.2. La entidad cuenta con una política definida que determine el uso, la protección y ciclo de vida de las claves criptográficas.			X
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.			

A.11.1. La entidad usa control de acceso físico a los perímetros donde se maneja información crítica o hacia instalaciones que manejen información con el fin de prevenir el daño, la interferencia o acceso no autorizado.		X	
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.11.1.2. La entidad maneja o tiene definida áreas seguras, con controles de acceso adecuados que permitan acceso solo a personal autorizado.		X	
A.11.1.3. La entidad cuenta o tiene definido un esquema de seguridad física para oficinas, salas e instalaciones.		X	
A.11.1.4. La entidad cuenta con un diseño físico que permita la protección física contra accidentes, ataques maliciosos o desastres naturales.		X	
A.11.1.5. La entidad tiene definido un protocolo o procedimiento para realizar trabajos en áreas seguras.			
A.11.1.6. La entidad hace o tienen control en los puntos donde circula personal no autorizado como en las áreas de descarga.			X
A.11.2 Equipos			
A.11.2.1 La entidad tiene definido un procedimiento que proteja de perdida, daño,		X	

robo o compromiso los activos de la alcaldía y la continuidad de las actividades en la misma.			
A.11.2.2. La entidad cuenta con mecanismos de protección contra fallas de potencia o cualquier falla generada por interrupción en los servicios públicos que les soportan.		X	
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.11.2.3. El cableado eléctrico y de telecomunicaciones en la entidad cumple con la normatividad vigente que protege contra interferencias, interceptación o daño,		X	
A.11.2.4. La entidad cuenta con un plan de mantenimiento de equipos que garantice la disponibilidad e integridad continua.			X
A.11.2.5. La entidad cuenta con un protocolo para el manejo o traslado de equipos, información o software de sus sitios de ubicación.		X	
A.11.2.6. La entidad tiene definido mecanismos o protocolos de seguridad para el manejo de equipos por fuera de las instalaciones de la misma.		X	
A.11.2.7. La entidad cuenta con un procedimiento para el manejo de equipos o elementos que almacenen información, garantizando que sean borrados o sobrescrito de forma segura antes de ser reusado.		X	

A.11.2.8. La entidad cuenta con medidas que garanticen la protección de los equipos cuando estos están sin supervisión del operador.		X	
A.11.2.9. La entidad cuenta con una política que permita el manejo de escritorio limpio de papeles en el puesto de trabajo y de pantalla limpia.			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.12. SEGURIDAD DE LAS OPERACIONES.			
A.12.1. La entidad cuenta con protocolos que garanticen la correcta realización de las operaciones en las áreas de procesamiento.		X	
A.12.1.1. La entidad cuenta con procedimientos operativos documentados y disponibles para los usuarios que los necesiten.		X	
A.12.1.2. La entidad tiene definidos mecanismos de control de cambios de manera que se registren y controlen los mismos en los procesos, en las instalaciones, y en los sistemas de procesamiento de datos que pueda afectar la seguridad de la información.		X	
A.12.1.3. La entidad realiza un seguimiento al uso de recursos, ajusta y proyecta los mismos para cubrir las necesidades futuras para el desempeño adecuado del sistema.		X	
A.12.1.4. La entidad cuenta con ambientes de desarrollo, ensayo y operativo separados con el fin de minimizar los riesgos de acceso o		X	

cambios no autorizados al sistema en operación.			
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.12.2.1. La entidad tiene implementado mecanismos de detección, prevención y recuperación, así como concientización de los usuarios operadores para proteger la información de códigos maliciosos.			X
A.12.3. La entidad tiene mecanismos de protección contra la pérdida de datos.		X	
A.12.3.1. La entidad maneja un protocolo para la realización de copias de seguridad y se ponen a prueba regularmente.		X	
A.12.4. La entidad lleva un registro de los eventos y genera evidencias de los mismos.			X
A.12.4.1. La entidad realiza una revisión periódica regular de los registros de los eventos de actividades del usuario, fallas, o incidentes de seguridad de información.			X
A.12.4.2. La entidad protege la información de los registros de los eventos que se generan.			X
A.12.4.3. La entidad lleva el registro de todas las actividades que realiza el administrador y			X

los operadores del sistema, estos se guardan y revisan con frecuencias regulares.			
A.12.4.4. La entidad tiene configurada la hora de los sistemas de procesamiento de información con una única zona horaria.		X	
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.12.5. La entidad tiene establecido un procedimiento para verificar la integridad del sistema.			X
A.12.5.1. La entidad establece algún procedimiento para controlar la instalación de programas o aplicaciones en sistemas operativos.		X	
A.12.6. La entidad tiene definido un procedimiento para prevenir el acceso por vulnerabilidades técnicas de los sistemas.			X
A.12.6.1. La entidad establece un procedimiento que permita conocer de forma oportuna las vulnerabilidades técnicas de los sistemas que usa, de manera que pueda valorar estos riesgos y se tomen acciones para mitigarlos.			X
A.12.6.2. La entidad tiene definida una política o procedimiento para reglamentar la instalación de software.		X	

A.12.7. La entidad realiza actividades de auditoria controladas y planificadas que permitan minimizar el impacto en los sistemas.			X
A.12.7.1. La entidad realiza auditoria sobre los sistemas operativos con el cuidado y la planificación que minimice interrupciones en las actividades.			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.13. SEGURIDAD DE LAS COMUNICACIONES.			
A.13.1. La entidad cuenta con mecanismos que protejan la red y las instalaciones de procesamiento.			X
A.13.1.1. La entidad cuenta con mecanismos que permitan gestionar y controlar la seguridad de la información de los sistemas y aplicaciones.			X
A.13.1.2. La entidad cuenta con mecanismos de seguridad, niveles de servicios y requisitos de gestión de los servicios de red identificados, de forma que los tiene incluidos en los acuerdos de servicios de red sean prestados internos o externamente.			X
A.13.1.3. La entidad tiene identificados y separados por grupos los servicios de información, usuarios y sistemas de información en la red.			X

A.13.2. La entidad tiene definido un procedimiento o mecanismos que brinde seguridad a la información que circula en la red o se intercambia con otra entidad externa.			X
A.13.2.1. La entidad tiene políticas, procedimientos y mecanismos de control formales para la transferencia de información en cualquier tipo de red de comunicación.			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.13.2.2. La entidad tiene definido acuerdos para la transferencia de información en la entidad o hacia cualquier parte externa.			X
A.13.2.3. La entidad usa mecanismos de protección para la información incluida en los correos electrónicos.			X
A.13.2.4. La entidad cuenta con acuerdos de confidencialidad documentados y los revisa regularmente para garantizar la protección de la información de acuerdo a las necesidades.			X
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.			
A.14.1. La entidad garantiza que la seguridad de la información es parte integral de los sistemas de información durante su ciclo de vida e incluido la prestación de servicios sobre redes públicas.			X
A.14.1.1. La entidad incluye y exige en los nuevos sistemas de información requisitos para mejorar la seguridad de los mismos.		X	

A.14.1.2. La entidad protege la información involucrada en servicios de aplicaciones que corren sobre medios de transmisión públicos con el fin de evitar accesos o modificaciones no autorizados.			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.14.1.3. La entidad protege los servicios de aplicaciones de manera que garantiza la integridad y la autenticidad de la información involucrada en las operaciones de comunicación y transmisión.			X
A.14.2. La entidad garantiza que La información generada en los sistemas informáticos se encuentra dentro del ciclo de vida de los mismos.			X
A.14.2.1. La entidad tiene definida políticas para el desarrollo de software en la alcaldía de San Antero.		X	
A.14.2.2. Existen procedimientos de control de cambios a los sistemas informáticos de la alcaldía.			X
A.14.2.3. La entidad tiene definido un procedimiento para verificación de las aplicaciones críticas luego de cambios de manera que no ocurran efectos adversos en la Alcaldía de San antero.			X

A.14.2.4. Se mantienen restringidos los cambios a los paquetes de software de acuerdo a las necesidades de la entidad.		X	
A.14.2.5. Se siguen las políticas de seguridad de la información para mantener el sistema protegido y con garantías de seguridad.		X	
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.14.2.6. La entidad garantiza que el ambiente de desarrollo se mantenga seguro.			X
A.14.2.7. La alcaldía lleva control y seguimiento a las actividades desarrolladas por terceros.		X	
A.14.2.8. La entidad realiza pruebas en ambientes controlados para probar la funcionalidad de los desarrollos.			X
A.14.2.9. la entidad establece periodos de pruebas a los sistemas nuevos en la alcaldía.			X
A.14.3.1. La entidad hace un buen tratamiento a los datos de ensayo para mantener la seguridad de estos.		X	
A.15. RELACIONES CON LOS PROVEEDORES.			
A.15.1. La entidad trabaja protege la información que es accedida por terceros o proveedores.		X	
A.15.1.1. La entidad tiene definida políticas para el manejo de información con proveedores en acuerdo con ellos.			X

A.15.1.2. La entidad tiene establecidos los requisitos de seguridad con los proveedores que acceden o manipulan herramientas de TI.			X
A.15.1.3. La entidad establece requisitos de seguridad y tratamiento de los riesgos que se puedan generar de las transacciones con los proveedores.			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.15.2. La entidad maneja o tiene definidos niveles de seguridad para los servicios en Línea en acuerdo con los proveedores.			X
A.15.2.1. La entidad hace seguimiento y control a los servicios prestados por los proveedores.			X
A.15.2.2. La entidad realiza hace gestión de cambios en actividades involucradas con terceros en cualquier área o servicio de TI.			X
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.			
A.16.1. Al presentarse incidentes de seguridad se comunica y da la atención oportuna y se emprenden actividades de mejora.			X
A.16.1.1. La entidad establece responsabilidades y pasos a seguir para dar una respuesta rápida y eficiente a los incidentes de seguridad.			X
A.16.1.2. La entidad informa a cerca de los incidentes de seguridad usando los canales de comunicación definidos para tal caso.		X	

A.16.1.3. La entidad establece todos los actores que interactúan con las herramientas de TI deben informar acerca de los incidentes o eventos detectados.		X	
A.16.1.4. La entidad evalúa los incidentes de seguridad y realiza la identificación de los mismos.			X
A.16.1.5. La entidad da respuesta a los incidentes de seguridad de acuerdo a los procedimientos documentados.			X
A.16.1.6. La entidad usa las experiencias de los incidentes para mejorar el impacto de los mismos en el futuro.		X	
A.16.1.7. La entidad tiene definido procedimientos para la preservación de evidencias de incidentes.			X
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO			
A.17.1. La entidad tiene definido mecanismos de continuidad del negocio dentro del proceso de seguridad de la información.			X
A.17.1.1. La entidad tiene establecido los requisitos de la seguridad de la información y su relación con la continuidad del negocio.			X
A.17.1.2. La entidad tiene definido y documentado los pasos a seguir para la seguridad de la información y continuidad del negocio.			X

A.17.1.3. La entidad realiaz control y seguimiento a los procedimientos definidos para la seguridad y continuidad del negocio de manera que se compruebe eficacia durante la ocurrencia de los mismos.			X
A.17.2. La entidad tiene equipos redundantes que permitan la continuidad de las actividades y la disponibilidad ante posibles eventualidades			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.18. CUMPLIMIENTO.			
A.18.1. La alcaldía establece los requisitos legales y contractuales según las leyes colombianas para sus procesos.		X	
A.18.1.1. Se identifican, documentan y mantienen al día con la normatividad establecida en Colombia para la seguridad de los sistemas informáticos.			X
A.18.1.2. La entidad establece mecanismos para garantizar los derechos de autor en el uso de herramientas de TI.		X	
A.18.1.3. La entidad protege los registros contra cualquier clase de daño de conformidad con la normatividad colombiana.			X
A.18.1.4. La alcaldía vela porque la información de sus usuarios y empleados se mantenga protegida y no llegue a ser de dominio público en conformidad con las leyes colombianas de protección de datos personales.			X

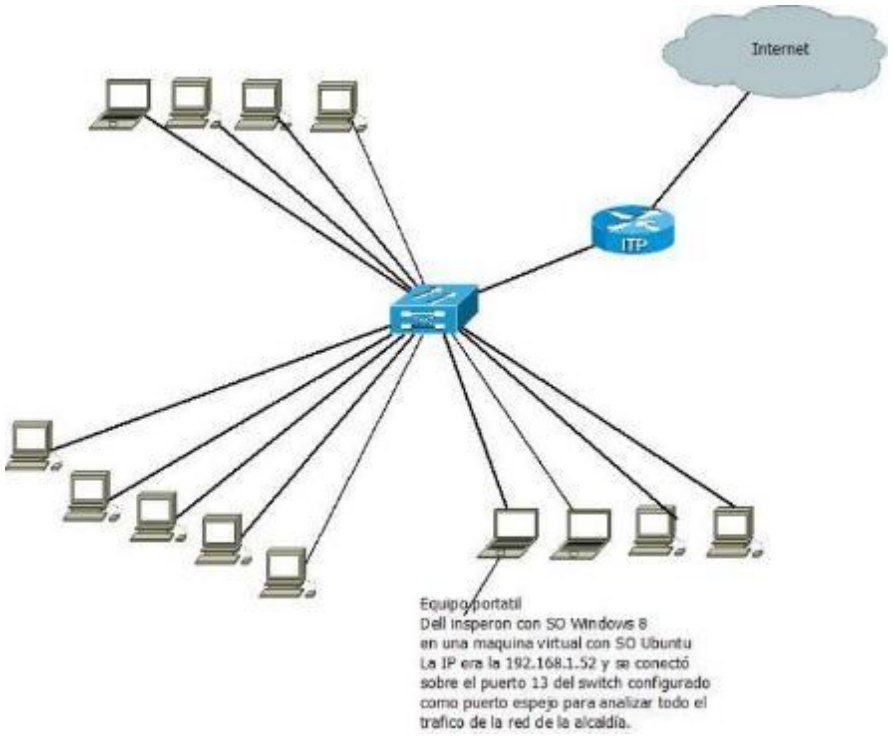
A.18.1.5. La entidad tiene definido el uso de controles criptográficos, en cumplimiento de todos los acuerdos.			X
A.18.2. La entidad controla que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimiento de la entidad.			X
OBJETIVOS DE CONTROL Y CONTROLES	Cumple a cabalidad	Cumple a parcialidad	No cumple
A.18.2.1. La entidad revisa sus procesos y procedimientos definidos para mantener la seguridad en periodos distintos a los planeados o cuando hay cambios.			X
A.18.2.2. Los directivos de la entidad revisan regularmente el cumplimiento de los procesamientos definidos para garantizar la seguridad.			X
A.18.2.3. La entidad realiza revisiones periódicas para determinar el cumplimiento con las políticas y normas de seguridad de la información.			X

Fuente: Autores

5.4.2 Secuencia de pantallas de las pruebas realizadas con herramientas para analizar el tráfico en la red de datos

La Alcaldía de San Antero cuenta con una red cableada Ethernet cuya topología es en estrella, donde existen unos nodos centrales “switches” que centralizan la conexión y generan una conexión punto a punto hasta estaciones de trabajo, lo cual la hace poco vulnerable a interrupciones generales o totales por daños entre estos.

Imagen 3 Topología de Red Alcaldía de San Antero con equipo de pruebas internas



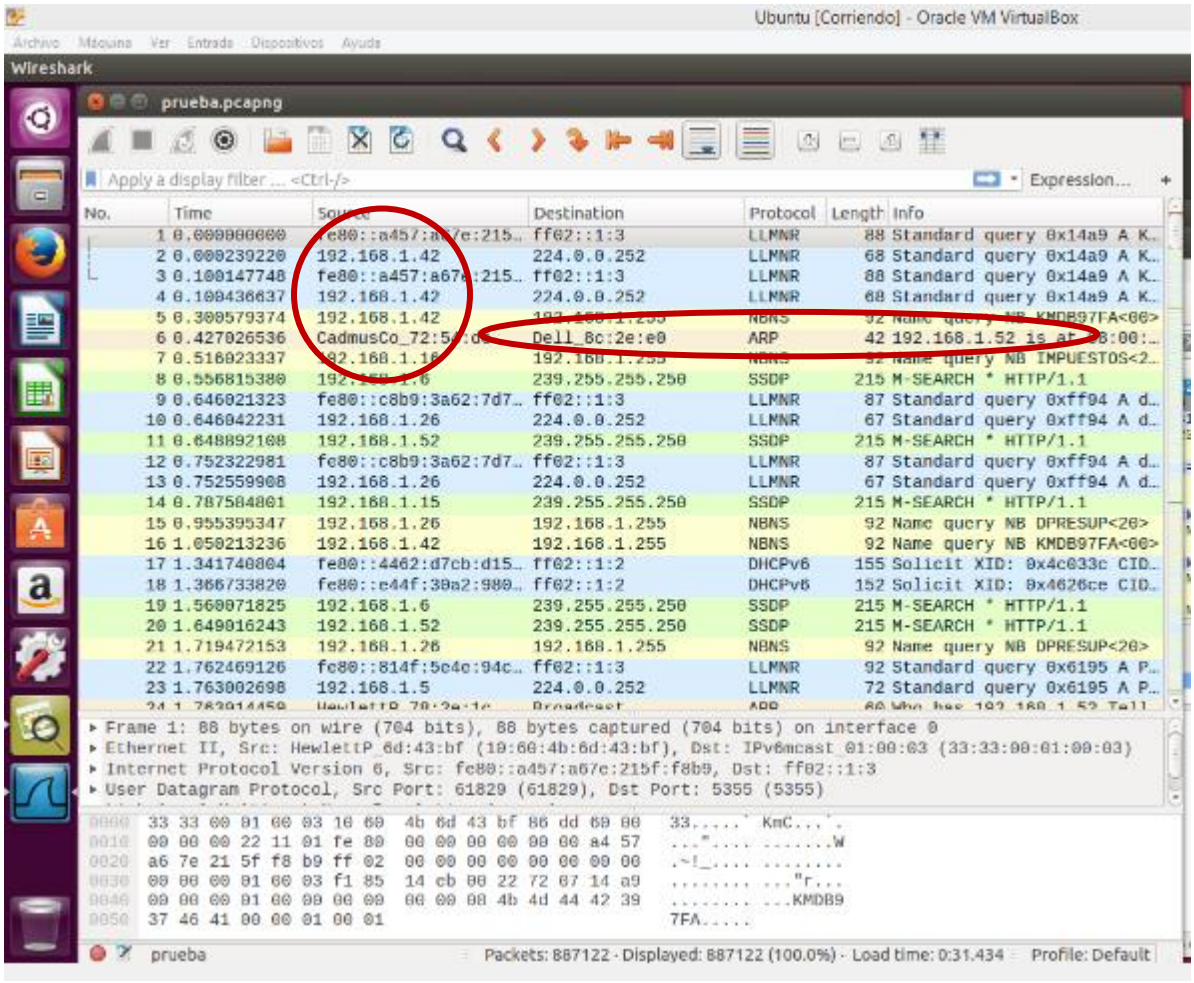
Fuente: Autores

Esta topología permite que el tráfico en la red se reparta y llegue al nodo de destino haciendo gestión de los paquetes al pasar por el nodo central “Switch”.

Las pruebas de tráfico se generaron desde equipos con máquinas virtuales con herramientas para enviar paquetes y analizar el tráfico en la red. En las siguientes imágenes encontramos la comunicación que establecen los diferentes equipos de la alcaldía, se pueden observar las direcciones IP abiertas, los protocolos utilizados,

los puertos de mayor frecuencia y las MAC de los equipos. Esta primera prueba fue realizada con la herramienta WireShark la cual solo necesita situar un equipo dentro de la red con IP privada 192.168.1.1 a 192.168.1.254 (la alcaldía no tiene la red interna en subredes) y el equipo DELL se le asignó la IP 192.168.1.52 conectado al puerto 13 switch, el cual funcionaba como puerto espejo para así poder detectar todo el tráfico de la red. Todo el análisis de tráfico que se realizó dentro de la red de la alcaldía se hizo con la configuración de la imagen 3, lo cual engloba a lo ejecutado en este punto 5.4.2.

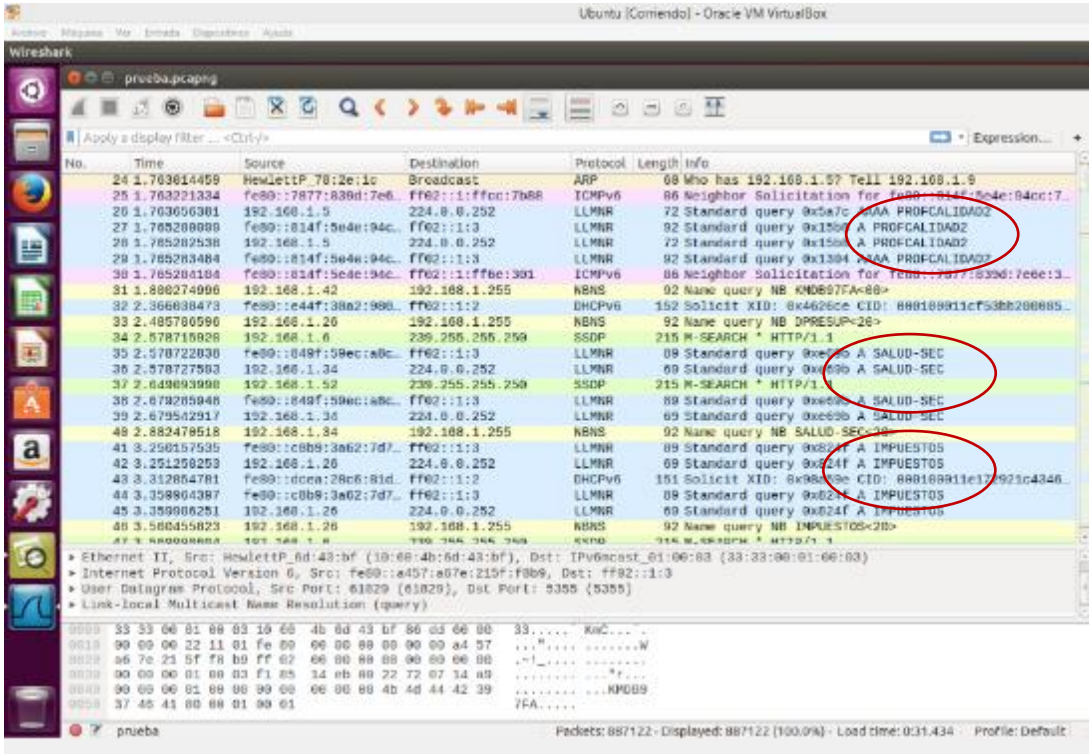
Imagen 4 Tráfico de Red en Alcaldía de San Antero Córdoba 1



Fuente: Autores

En el círculo rojo podemos observar las direcciones IP que están enviando información a diferentes destinatarios con los respectivos protocolos que permiten la comunicación de estos servicios. En el círculo más alargado de la imagen anterior se puede notar el equipo DELL que nos sirve para hacer Sniffing.

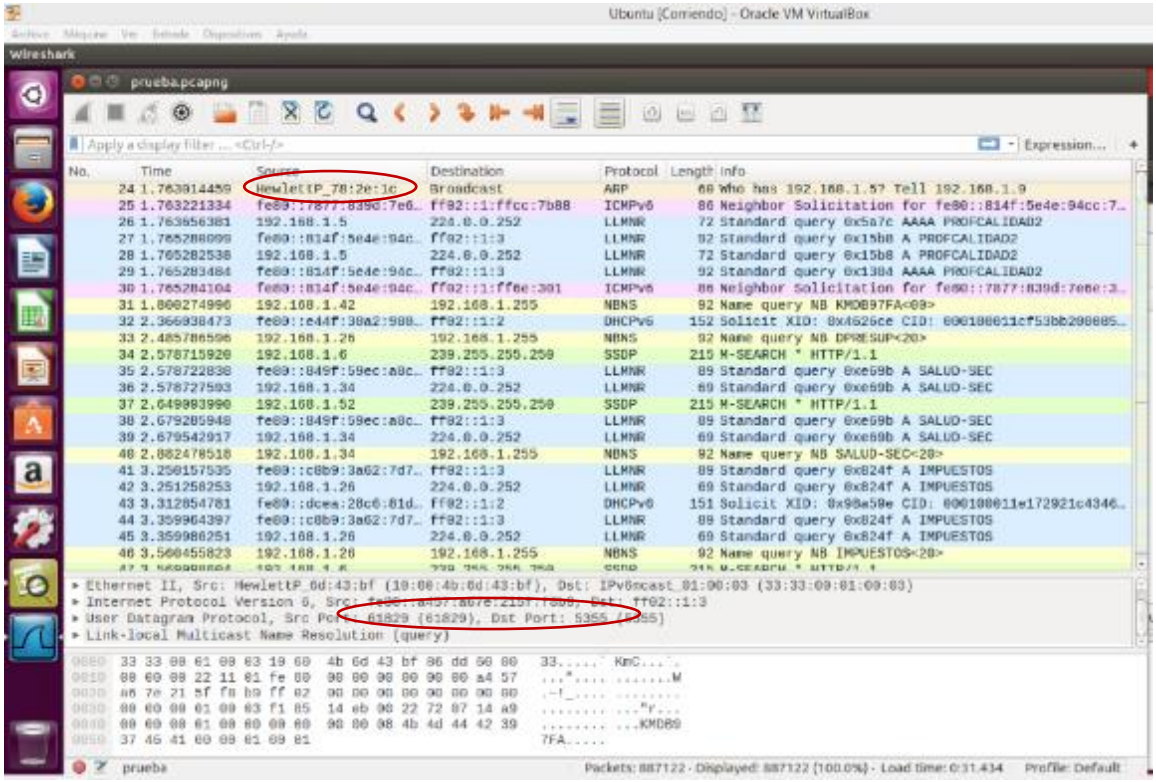
Imagen 5 Tráfico de Red en Alcaldía de San Antero Córdoba 2



Fuente: Autores

En esta imagen podemos detallar, en los círculos rojos, los departamentos que están estableciendo comunicación los cuales son críticos en el funcionamiento de la alcaldía debido a que pueden contener información sensible de usuarios de los servicios médicos que lidera la secretaría de salud, pago de impuestos y el departamento de calidad.

Imagen 6 Tráfico de Red en Alcaldía de San Antero Córdoba 3



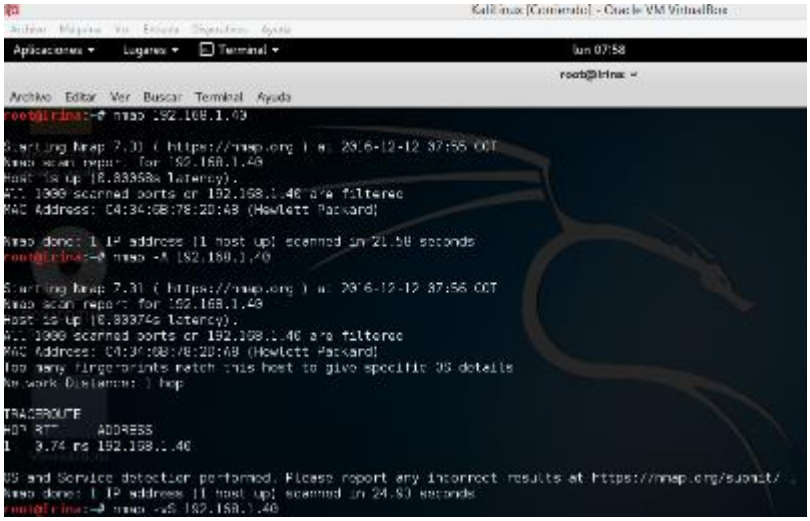
Fuente: Autores

En esta otra imagen detallamos los puertos de salida y la MAC de uno de los equipos que está estableciendo comunicación.

En las diferentes imágenes podemos destacar los protocolos que más usa la red para establecer comunicación, los cuales al identificar las direcciones IP y las MAC de los equipos hace visible las posibles vulnerabilidades a explotar.

Al ingresar dentro de la red y hacer un escaneo de los equipos de cómputo podemos recabar información personal tales como contraseñas, páginas que más se frecuentan, datos bancarios y más. Si un atacante tiene ingreso a la red sería algo muy riesgoso para la alcaldía.

Imagen 7 Resultado de Nmap a equipo con S.O w7 profesional



Fuente: Autores

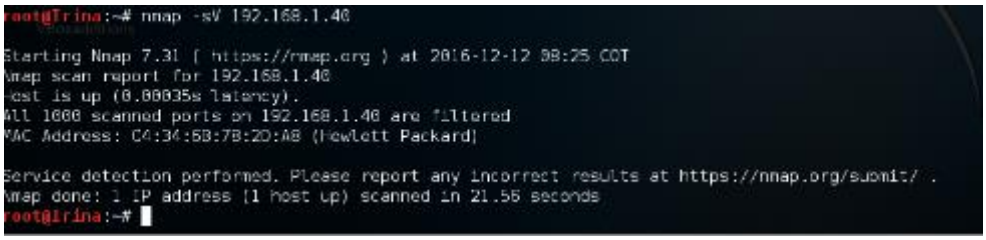
La anterior imagen es un escaneo hecho de forma interna a un equipo de la alcaldía. Se utilizó el mismo equipo marca DELL pero con otra máquina virtual con SO Kali Linux y por terminal se hizo un análisis de la IP 192.168.1.40 con la herramiena Nmap.

Imagen 8 Escaneo con nmap a Router del ISP de Alcaldía de San Antero Córdoba

Fuente: Autores

En esta imagen se puede evidenciar la marca del router, los puertos abiertos y sus respectivos servicios

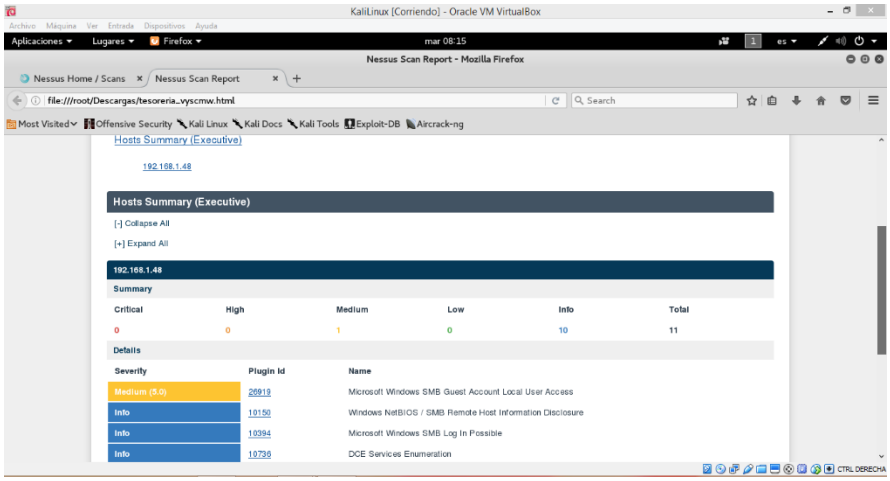
Imagen 9 Escaneo de puertos red interna con Nmap



Fuente: Autores

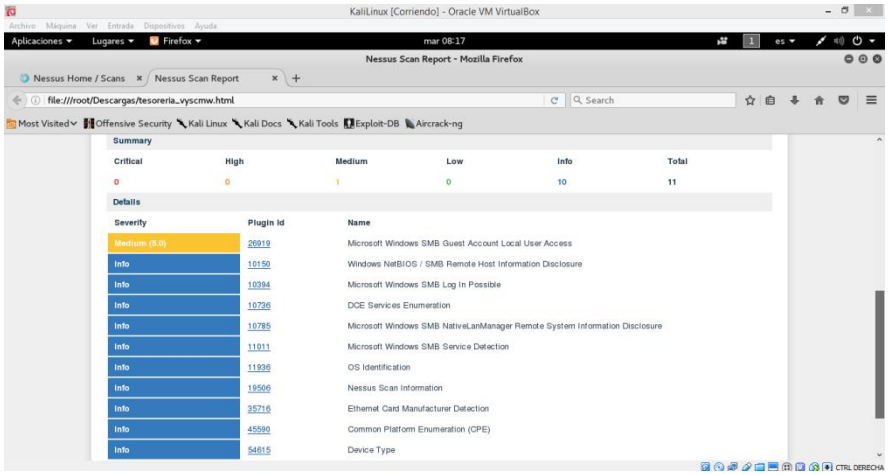
Esta imagen detalla que la IP analizada tiene los puertos filtrados

Imagen 10 Pruebas a equipos de la red interna desde Nessus



Fuente: Autores

Imagen 11 Resultado escaneo con Nessus



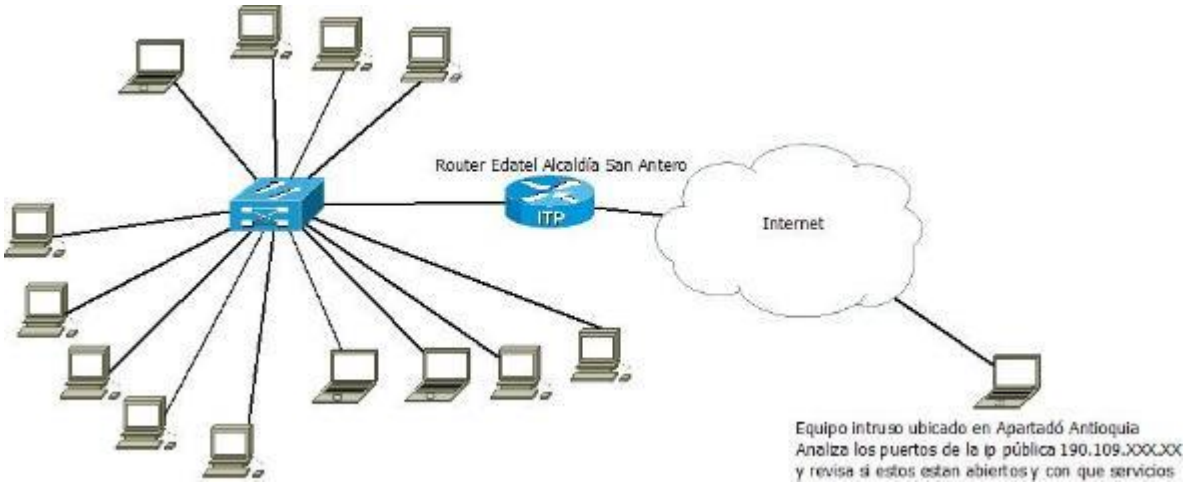
Fuente: Autores

El resultado del scaneo con Nessus no muestra ninguna vulnerabiliad crítica o alta. Solo muesra una ulnerabilidad media indicando que uno de los equipos tiene los servicios de SAMBA abiertos.

5.4.3 Secuencia de pantallas de las pruebas realizadas con herramientas para analizar vulnerabilidades de la red en un equipo remoto

Las imágenes que se muestran a continuación fueron desarrolladas a partir de una de las direcciones IP de la alcaldía de San Antero Córdoba en la cual se puede apreciarlas características del equipo y los puertos que tienen abierto. Al igual que NMAP esta herramienta solo hace un análisis de los servicios que tiene la red en sus diferentes puertos, pero no hace ningún ataque.

Imagen 12 Topología de red Alcaldía de San Antero con equipo remoto de pruebas

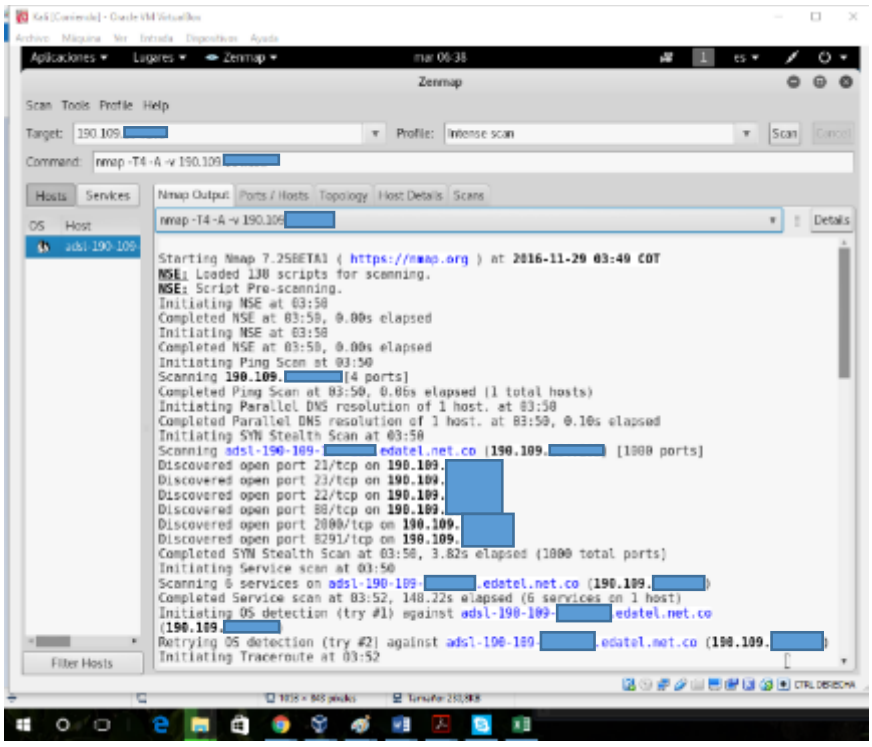


Fuente: Autores

Esta imagen es la topología de red para las pruebas realizadas de forma remota sobre la IP pública de la alcaldía 190.109.XXX.XXX, en el que se exploraron los puertos abiertos y los servicios que están abiertos en esos puertos. Las pruebas se hicieron en un equipo portátil Acer Aspire E5 con SO Windows 10 y las pruebas virtuales se desarrollaron sobre máquina virtual usando Kali Linux

ZENMAP

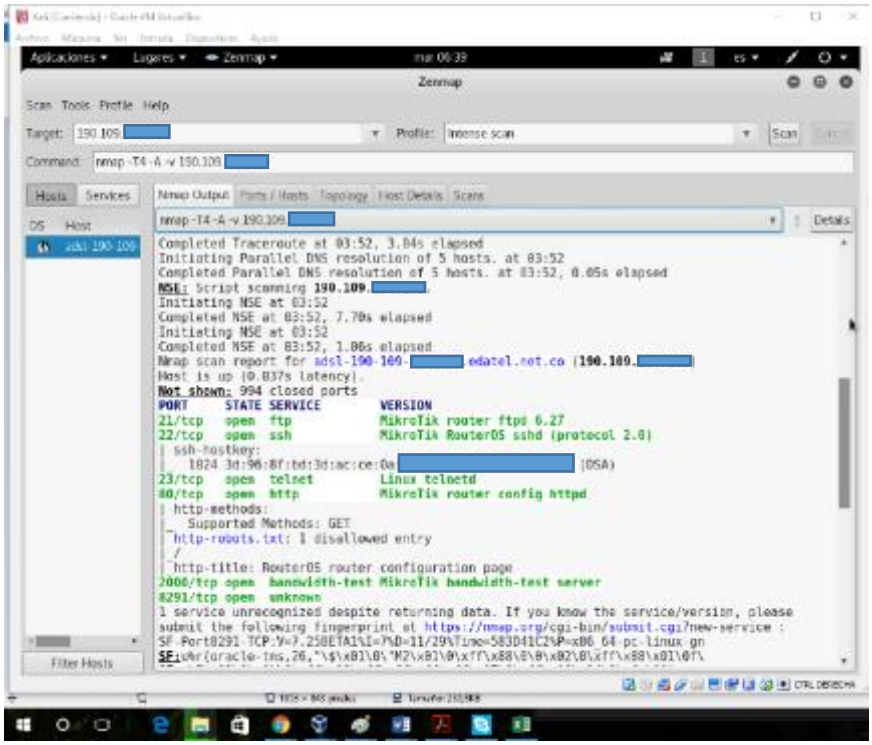
Imagen 13 Escaneo a IP fija del servicio de Internet



Fuente: Autores

Aquí se muestran los puertos que están abiertos del router que provee los servicios de red a la Alcaldía

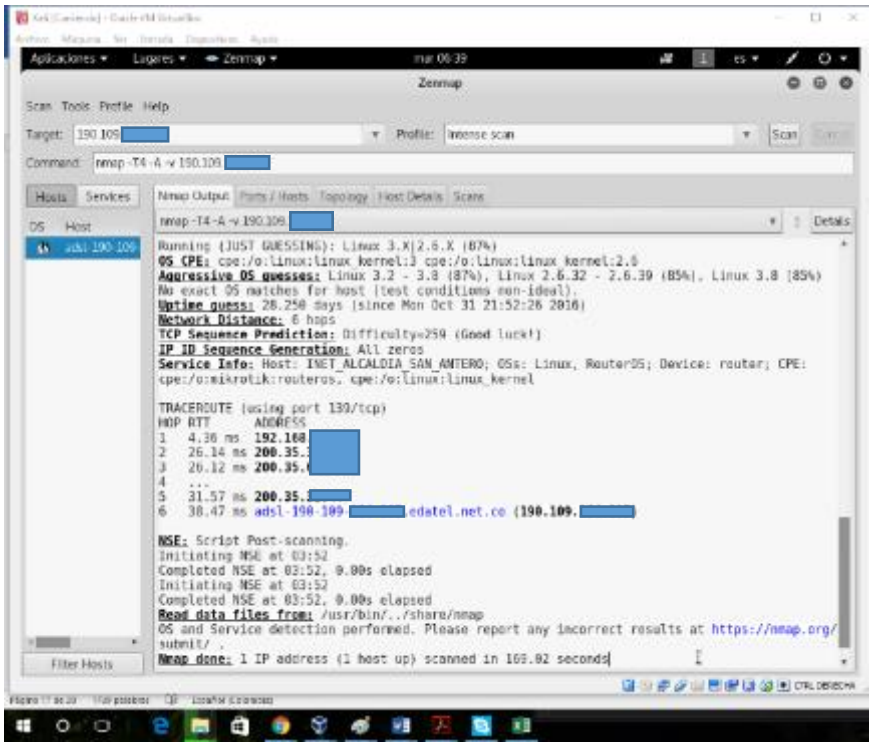
Imagen 14 Resultado escaneo a IP fija del servicio de Internet



Fuente: Autores

En esta imagen no solo observamos los puertos abiertos, también podemos ver el Router de la alcaldía que posibilita los servicios de Internet. Con los puertos abiertos y su respectiva IP se podrían presentar ataques del tipo Man-in-the-middle.

Imagen 15 Ruta escaneo a IP fija del servicio de Internet

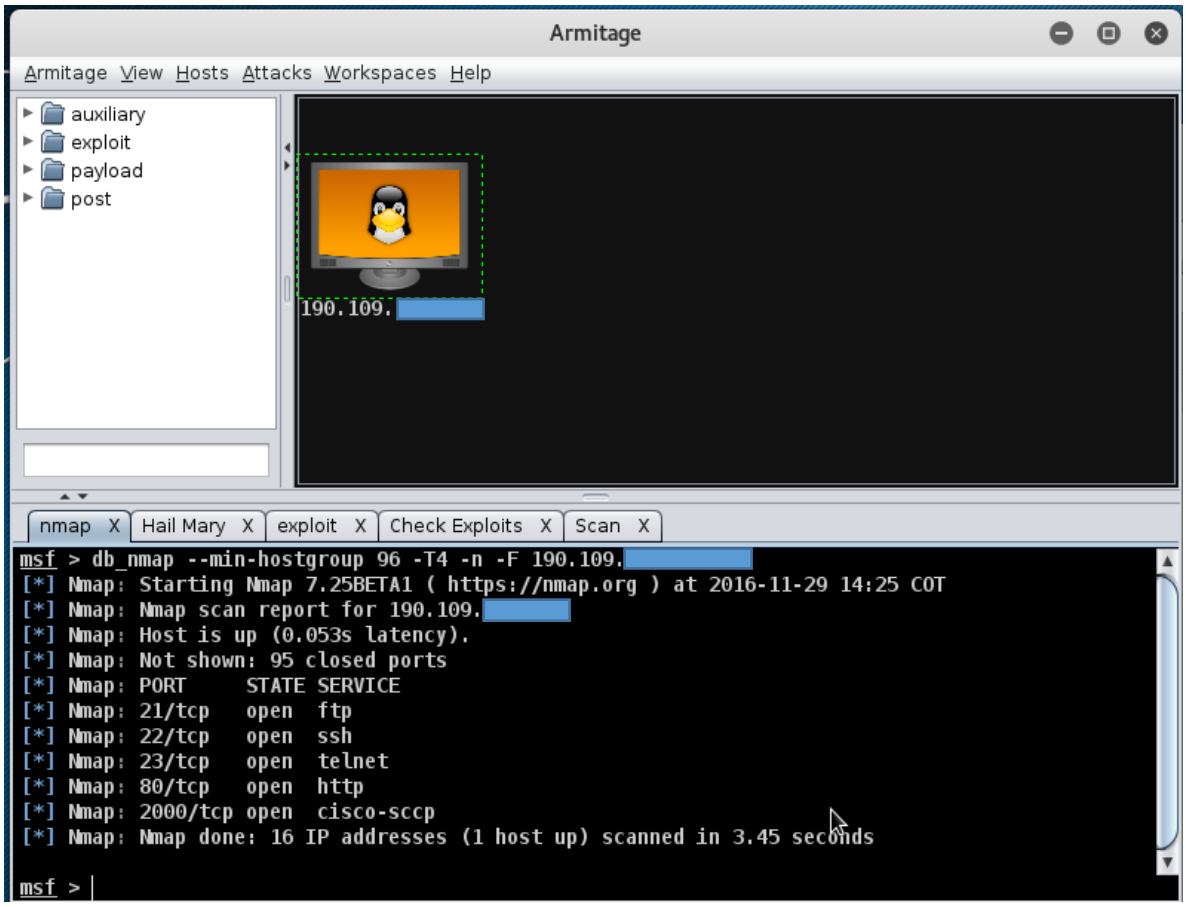


Fuente: Autores

En esta última se observa la ruta que se tomó para establecer comunicación con el Router de la alcaldía el cual muestra que la proveedora de servicios es Edatel.

A continuación, se muestra la realización de una prueba con la herramienta Armitage, el cual es similar a ZENMAP pero con el adicional que esta herramienta nos permite explotar vulnerabilidades.

Imagen 16 Escaneo a ip Fija del servicio de internet con Armitage



Fuente: Autores

Con esta herramienta no solo observamos los servicios que se pueden explotar, también podemos dirigir ataques a los diferentes puertos que están abiertos o hacer un análisis de las vulnerabilidades que tiene la red. Esta prueba también se hizo de forma remota al Router de la alcaldía.

5.4.4 Identificación de Vulnerabilidades, Amenazas, valoración del Riesgo y análisis de riesgos bajo metodología Magerit

La metodología Magerit va a permitir hacer la gestión del riesgo, para tomar decisiones teniendo en cuenta riesgos que pueden presentarse del uso de TI, se basa en el análisis del impacto que puede tener en una organización la violación de la seguridad de la información, buscando detectar las posibles amenazas y vulnerabilidades que terceros podrían explotar, con el fin de tomar medidas preventivas y correctivas eficaces. Aplicamos esta metodología con la finalidad de hacer un seguimiento a las posibles situaciones que pudieran presentarse en la Alcaldía de San Antero y de esta forma tratar de mitigar los riegos de situaciones que no se escapan al control humano.

Tabla 3 Valoración de Activos

Código	Activo	Confidencialidad	Disponibilidad	Integridad	Autenticidad	Trazabilidad	Total
SU01	Servidor de usuarios	3	5	5	3	3	4
BD01	Base de datos Sistema de impuesto predial SIMPU	4	5	5	5	5	5
BD02	Base de datos Sistema integrado de información SIIM	4	5	5	5	5	5
BD03	Base de datos Sistema de industria y comercio SINCO	4	5	5	5	4	5
CP01	Computadores	3	5	5	2	3	4
ER01	Equipos de red	3	5	5	2	3	4

Fuente: Autores

Escala estándar

Tabla 4 Escala de daños y criterios

5 - A	Daño extremadamente grave
4 - M+	Daño muy grave
3 - M	Daño grave
2 - M-	Daño importante
1 - B	Daño menor
Criterios Que Valorar	
C	Confidencialidad
I	Integridad
D	Disponibilidad
A	Autenticidad
T	Trazabilidad

Fuente: Autores

Tabla 5 Valoración del riesgo

Dimensión: Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad				**Valoración del Riesgo**				
Activo	**Vulnerabilidades**	**Amenazas**	**Riesgos**	**Criterios**				
				C	**I**	**D**	**A**	**T**
Software	Falta de capacitación en el manejo de Prevención y desastres	Incendio producido por Falla Humana (accidental o deliberado)	Pérdida de Información crítica e interrupción en la continuidad del Negocio.	2	2	5	3	2
		Incendio Por causas naturales (rayo, tormenta eléctrica, terremoto, ciclones)		2	2	5	1	2

		Inundaciones causadas por Lluvias		2	2	5	1	2
		Inundaciones por fugas, escapes, en tuberías, producido por Falla Humana (accidental o deliberado)		2	2	5	1	1
		Explosiones, desplomes en instalaciones,		1	1	5	1	2
	Falta de Control y seguimiento a los sistemas eléctricos	Sobrecarga eléctrica	Daño en equipos y dispositivos de hardware sensibles	1	5	5	3	5
		Fluctuaciones eléctricas		1	5	5	5	3
	Falta de capacitación en el personal de servicios Generales	Contaminación mecánica por polvo y suciedad accidental o deliberada	Recalentamiento y daño físico en equipos y dispositivos de hardware	1	2	2	2	2
	Falta de un Plan de Mantenimiento preventivo para equipos de Hardware	Fallos en los equipos de computadoras/servidor y/o fallos en los programas por causas físicas o lógicas.	Perdida de Información crítica e interrupción en la continuidad del Servicio	5	4	4	4	3
	Falta de Verificación y Seguimiento de continuidad a los circuitos de Energía Regulados	Fallos en los sistemas y en los equipos por corte inesperado del fluido eléctrico.	Daño en equipos y dispositivos de hardware sensibles	1	4	4	4	2

	Falta de condiciones de aireación en las instalaciones	Fallos en los sistemas y en los equipos por condiciones inadecuadas de temperatura.		1	2	2	4	2
	Falta de Plan de mantenimiento al sistema de Cableado Estructurado	Fallos en la red de comunicaciones por destrucción o daño en medios físicos o dispositivos de la red.	Interrupción en la continuidad del servicio	1	4	4	4	3
	Falta de actualización y repotenciación de Equipos y dispositivos de Hardware y software	Caída del sistema de información por deficiencia y agotamiento en los recursos y dispositivos.	Obsolescencia de Equipamiento informático (hardware y software)	1	1	5	4	4
	Falta de Capacitación o Actualización al Personal del área de sistemas	Errores en la configuración y programación	Debilidad en la seguridad Informática de la Entidad, generación de vulnerabilidades	1	1	4	3	4
Servicios	Falta de plan de contingencia	Interrupción en los servicios por fallos en los sistemas y en los equipos por corte inesperado del fluido eléctrico.	Perdida de Información crítica e interrupción en la continuidad del Servicio	1	1	3	3	1
	Falta de condiciones de aireación en las instalaciones	Interrupción en los servicios por fallos en los sistemas y en los equipos por condiciones inadecuadas de temperatura.		1	2	4	2	2

	Falta de Plan de mantenimiento al sistema de Cableado Estructurado	Interrupción en los servicios por fallos en la red de comunicaciones por destrucción o daño en medios físicos o dispositivos de la red.	Interrupción en la continuidad del servicio	1	1	5	4	3
	Falta de Planificación en la elaboración del Plan de Adquisiciones	Interrupción en los servicios por falta de recursos de consumo e insumos (tóner, papel)		1	1	1	4	3
	Falta de Mecanismos y dispositivos para agregar seguridad en los elementos de Software y Hardware	Suplantación de identidad	Pérdida de Información crítica e interrupción en la continuidad del Servicio, acceso no autorizado a los sistemas de información.	5	5	5	3	4
	Falta de capacitación den el personal a cargo de implementar seguridad lógica y física en hardware y software							
Servicios	Falta de políticas de seguridad y aplicación de buenas prácticas de TI.	Interrupción en el servicio por propagación de Malwares, troyanos, gusanos, Backdoors, etc.	Perdida de información crítica y acceso no autorizado.	5	5	5	3	5
	Fallas al escoger el proveedor del servicio	Interrupción del servicio por caída del canal de datos	Interrupción en la continuida	1	1	4	4	3

	Falta de seguimiento y auditoría a los procedimientos automatizados	Interrupción del servicio por fallas en la programación del software interno.	d del servicio	1	1	5	4	4
	Fallas al escoger el proveedor del servicio	Interrupción del servicio por lentitud en la respuesta del equipo de soporte en las aplicaciones internas.		1	1	5	4	4
	Falta de capacitación y motivación en el personal encargado	Interrupción en el servicio por error humano en la digitación y actualización de datos.	Daño a la reputación e imagen corporativa	5	5	1	5	4
Equipamiento Informático	Falta de capacitación en el manejo de Prevención y desastres	Daños por incendio producido por Falla Humana (accidental o deliberado)	Perdida de información crítica y acceso no autorizado.	1	4	5	4	3
		Incendio Por causas naturales (rayo, tormenta eléctrica, terremoto, ciclones)	Interrupción en la continuidad del servicio	1	1	5	2	1
		Daños por inundaciones causada por Lluvias		1	1	5	2	2
		Daños por Inundaciones por fugas, escapes, en tuberías, producido por Falla Humana (accidental o deliberado)		1	1	5	2	1
		Daños por Explosiones, desplomes en instalaciones	Daño a la reputación e imagen corporativa	1	1	5	1	2
	Falta de Control y seguimiento a los	Daños por Sobrecarga eléctrica	Daño físico en	1	1	5	5	4

	sistemas eléctricos	Daños por Fluctuaciones eléctricas	dispositivos de hardware sensibles a cambios eléctricos, Perdida de Información y recursos	1	1	5	5	4
		Daños en los sistemas y en los equipos por corte inesperado del fluido eléctrico.		1	1	5	5	4
Equipamiento Informático	Falta de capacitación en el personal de servicios Generales	Daños por Contaminación mecánica por polvo y suciedad accidental o deliberada	Recalentamiento y daño físico en equipos y dispositivos de hardware	1	1	5	3	3
	Falta de Aireación en las instalaciones	Daños en los sistemas y en los equipos por condiciones inadecuadas de temperatura		1	1	5	3	3
	Falta de un Plan de Mantenimiento preventivo para equipos de Hardware	Daños en los equipos de computadoras/servidor por falta de mantenimientos preventivos periódicos	Perdida de Información crítica e interrupción en la continuidad del Servicio	3	1	4	4	4
		Daños por desgaste en el tiempo del hardware de los equipos y dispositivos	Obsolescencia de Hardware y Baja capacidad de procesamiento	1	1	5	4	3
Personal	Falta de Esquema de comunicación	Indisponibilidad de usuario en puesto de trabajo: por enfermedad, alteraciones del orden público, etc.	Interrupción del servicio	1	1	5	3	5

	Falta de controles y mecanismos de Seguridad y Prácticas de TI	Manipulación de los sistemas de Información no autorizados	Perdida de Información crítica e interrupción en la continuidad del Servicio	5	5	5	3	3
		Manipulación en las configuraciones de forma intencional		5	5	5	3	3
		Suplantación de identidad		5	5	5	1	3
		Ataque destructivo de forma intencional		5	5	5	5	3
		Ingeniería social (abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.)		5	5	5	2	3
Software	Falta de capacitación	Errores del usuario cuando hace uso del sistema de Información.	Actualización errónea de Datos y deficiente prestación del servicio	1	1	1	4	4
	Falta de conocimiento o errores de configuración	Error del usuario administrador del sistema de información cuando usa o define parámetros en el sistema.	Accesos no autorizados al sistema, perdida de información	4	4	4	3	4
	Falta de políticas, buenas prácticas TI y Plan de Seguimiento y control de procesos y procedimientos.	Falta de mecanismos y rutinas de registro de actividad de los usuarios para seguimiento y trazabilidad del sistema de información.	Evasión de Responsabilidades y controles de los procedimientos	1	5	3	4	4

		Propagación de software dañino (propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.) por usuarios internos.	Destrucción de información o perdida de la misma	5	5	5	3	4
		Fugas de información por indiscreción del usuario, Suplantación de identidad /accesos no autorizados		5	4	4	3	4
	Falta de conocimiento o errores de configuración	Error de mantenimiento o actualización de los sistemas de información	Inestabilidad del sistema e interrupción del servicio	2	1	4	2	3
		Abuso de privilegios de acceso	Accesos no autorizados al sistema, perdida de información	5	4	5	2	4
		Usos no previstos (consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.)						
Servicios	Falta de capacitación para prestar el servicio	Errores del usuario cuando hace uso del sistema de Información y brinda el servicio	Actualización errónea de Datos y deficiente prestación del servicio	1	1	2	4	3
	Falta de conocimiento o errores de configuración	Error del usuario administrador del sistema de información cuando usa o define parámetros en el sistema, Suplantación de identidad, Abuso de Privilegios	Accesos no autorizados al sistema, perdida de información	5	4	4	3	4

	Falta de políticas, buenas prácticas TI y Plan de Seguimiento y control de procesos y procedimientos.	Falta de mecanismos y rutinas de registro de actividad de los usuarios para seguimiento y trazabilidad del sistema de información.	Evasión de Responsabilidades y controles de los procedimientos	5	4	4	4	3
		Propagación de software dañino (propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.) por usuarios internos.	Destrucción de información o perdida de la misma	5	4	5	4	3
		Fugas de información por revelación o indiscreción, Incontinencia verbal, medios electrónicos, soporte papel, etc		5	5	5	2	2
	Falta de conocimiento o errores de configuración	Falla en el servicio por caída del sistema de información por deficiencia y agotamiento o saturación en los recursos y dispositivos	Inestabilidad del sistema e interrupción del servicio	1	1	4	4	3
		Falla en el servicio por pérdida de equipos y soportes de información por sustracción de los mismos.	Accesos no autorizados al sistema, perdida de información	5	5	4	4	5

Fuente: Autores

Tabla 6 Análisis de riesgos

Matriz de Análisis de Riesgo — **Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]**

Actos originados por la criminalidad común

Aplicación de software, datos, hardware	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor
		4	1	3	4	3	3	3	4	3
Sistema Integrado de Información (SIIM)	4	16	4	12	16	12	12	12	16	12
Sistema de Impuesto predi	4	16	4	12	16	12	12	12	16	12

Sucesos de origen físico

Aplicación de software, datos, hardware	Magnitud de Daño	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
		2	3	2	3	1	2	1	1	4
Sistema Integrado de Información (SIIM)	4	8	12	8	12	4	8	4	4	16
Sistema de Impuesto predi	4	8	12	8	12	4	8	4	4	16

Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

Aplicación de software, datos, hardware	Magnitud de Daño	Falta de inducción, capacitación y sensibilización sobre	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar,	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del	Falta de mantenimiento físico (proceso, repuestos e	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el	Falta de mecanismos de verificación de normas y reglas /
		3	3	4	2	4	4	4	4	4	4	4	4	4	2	4	2	3	4	4	4	1	1	1	2	2
Sistema Integrado de Información (SIIM)	4	12	12	16	8	16	16	16	16	16	16	16	16	16	8	16	8	12	16	16	16	4	4	4	8	8
Sistema de Impuesto predi	4	12	12	16	8	16	16	16	16	16	16	16	16	16	8	16	8	12	16	16	16	4	4	4	8	8

al Unificado (SIMPU)																																													
Sistema de Industria y Comercio (SINCO)	4	16	4	12	16	12	12	12	16	12	8	12	8	12	4	8	4	4	16		12	12	16	8	16	16	16	16	16	16	16	16	16	8	16	8	12	16	16	16	4	4	4	8	8
Sistema de Inventario Municipal (INVEM)	4	16	4	12	16	12	12	12	16	12	8	12	8	12	4	8	4	4	16		12	12	16	8	16	16	16	16	16	16	16	16	16	8	16	8	12	16	16	16	4	4	4	8	8
Sistema de nómina municipal	4	16	4	12	16	12	12	12	16	12	8	12	8	12	4	8	4	4	16		12	12	16	8	16	16	16	16	16	16	16	16	16	8	16	8	12	16	16	16	4	4	4	8	8
Licencias de Sistema Operativo	3	12	3	9	12	9	9	9	12	9	6	9	6	9	3	6	3	3	12		9	9	12	6	12	12	12	12	12	12	12	12	12	6	12	6	9	12	12	12	3	3	3	6	6
Web Institucional	1	4	1	3	4	3	3	3	4	3	2	3	2	3	1	2	1	1	4		3	3	4	2	4	4	4	4	4	4	4	4	4	2	4	2	3	4	4	4	1	1	1	2	2
Correo Electrónico	2	8	2	6	8	6	6	6	8	6	4	6	4	6	2	4	2	2	8		6	6	8	4	8	8	8	8	8	8	8	8	8	4	8	4	6	8	8	8	2	2	2	4	4
Servidor	4	16	4	12	16	12	12	12	16	12	8	12	8	12	4	8	4	4	16		12	12	16	8	16	16	16	16	16	16	16	16	16	8	16	8	12	16	16	16	4	4	4	8	8

Equipos de computo	2	8	2	6	8	6	6	6	8	6	4	6	4	6	2	4	2	2	8		6	6	8	4	8	8	8	8	8	8	8	8	8	4	8	4	6	8	8	8	2	2	2	4	4
Equipos de red	4	16	4	12	16	12	12	12	16	12	8	12	8	12	4	8	4	4	16		12	12	16	8	16	16	16	16	16	16	16	16	16	8	16	8	12	16	16	16	4	4	4	8	8

5.5 CRONOGRAMA

Las Actividades Realizadas para la organización de esta propuesta de proyecto de grado están enmarcadas así: Trabajo con cronograma en semanas.

Tabla 7 Cronograma de Actividades

Meses	Junio			Julio				Agosto				sept				Oct				Nov				Dic			
Actividad	S1	S2	S3	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S1	S2	S3	S4	S1	S2	S3	S4	S1
Elaboración de idea y entrega de propuesta proyecto																											
Levantamiento de información y estado de arte																											
Análisis de Información levantada																											
Entrega de la propuesta para pre aprobación																											
Entrega de correcciones de la propuesta luego de ajustes																											

Determinación de Herramientas y métodos de diagnóstico de controles y de la seguridad en la red de datos	
Determinación de Recursos	
Realización de Pruebas a la red de datos	
Recolección y Registro de Datos de las Pruebas del monitoreo y seguimiento a la red de datos	
Realización de Análisis a los Datos recolectados	
Elaboración y entrega del documento propuesta solución	
Realización de Ajustes después de Revisión a propuesta solución	
Entrega de documento final propuesta solución	

Fuente: Los Autores

6 RESULTADOS Y DISCUSIÓN

Después del respectivo análisis a las vulnerabilidades en la alcaldía de San Antero Córdoba, las recomendaciones están más orientadas al trabajo que se debe hacer desde lo administrativo debido a que con el análisis se puedo encontrar que los sistemas están relativamente bien, no tienen software ilegal en sus equipos lo que permite que siempre tengan las actualizaciones. Los equipos que manejan las actividades críticas tienen antivirus con licencias pagadas y los otros gratuitos. A nivel lógico el sistema presenta protección. Sumado a que la red de internet de la alcaldía no se conecta ninguno de sus equipos vía WIFI, más bien todo el sistema es cableado y se encuentra en lugares que hacen difícil para algún extraño intentar ingresar al sistema.

Sin embargo, según los controles basándonos en la norma ISO 27001:2013 se detecta la necesidad de implementación de un SGSI, el cual es fundamental debido a que permite Planificar, Hacer, Verificar y Actuar, pero al momento de redactar estas conclusiones todavía la alcaldía no ha hecho gestión para la implementación del mismo.

- ✓ De acuerdo a la serie de pruebas realizadas hasta el momento no se han encontrado vulnerabilidades críticas en los equipos rastreados, dando una imagen de que el proceso de filtro está bastante bien configurado, dado que el accesos a la Internet en su mayoría se realiza para el manejo de servicios como el correo electrónico y consultas, sin un grado amplio de transacciones en línea en ambientes interoperables que interactúen y comprometan los servicios y equipos internos directamente durante una transacción, en este sentido se debe enfocar las acciones de mejoramiento del sistema telemático hacia el desarrollo e implementación de un SGSI el cual permita hacer una identificación más puntual y detallada que organice e identifique los procesos y procedimientos de las áreas críticas y defina mecanismos de control y

políticas de seguridad de la información. Así como el desarrollo integral del recurso humano como elemento importante y vulnerable por omisión o desconocimiento de forma que se pueda llevar y crear un proceso integrado de conocimiento y cultura de seguridad en la entidad. Hasta el punto que el actor interno respete las políticas, procedimientos y aspectos de seguridad, hasta convertirlo en un hábito y lo apliquen a cada instante en la entidad y porque no en su vida cotidiana.

Para disminuir así la brecha entre el desconocimiento y la conciencia de aplicación de buenas prácticas de TI en la Alcaldía de San Antero Córdoba.

- ✓ Las decisiones administrativas deben ser complementadas en aspectos de seguridad y privacidad de la información, es necesario implementar seguridad perimetral con el fin de contrarrestar el acceso de actores no autorizados mediante dispositivos activos en la red, como firewalls, UTMS, proxys, sistemas de detección de intrusos.

- ✓ Así mismo se sugiere la segmentación de red para que se distribuya seguridad de acuerdo a la criticidad de los segmentos en la red interna mediante la limitación de los accesos y el tráfico interno entre áreas y recursos críticos que maneja la entidad. Esta medida puede permitir dar un mejor uso al ancho de banda y mejorarían los tiempos de respuesta en los sistemas de información internos que brindan servicios críticos con necesidad de tiempos de respuestas óptimos para la realización de transacciones locales.

- ✓ La conectividad y los servicios críticos requieren tener un respaldo tanto para el canal como para los sistemas de información y servicios dado que no se cuenta con copias espejos o un servicio en la nube que garanticen la continuidad con tiempos de respuesta aceptables en caso de un incidente u ocurrencia de un riesgo, lo cual es fundamental para mantener los servicios.

- ✓ Así mismo se recomienda la implementación de un sistema de gestión de red que permita tener el control local o remoto de los distintos dispositivos en la red de datos y poder hacer un continuo monitoreo y control de la misma.

- ✓ Se recomienda realizar un plan de contingencia, que contenga las políticas, la organización, los procedimientos y métodos, necesarios para enfrentar una emergencia o desastre cuando exista falla grave en la red o en los sistemas y equipos activos críticos de la misma.

- ✓ Es necesario crear manuales de configuración y administración para todos los dispositivos activos críticos de la infraestructura de red de datos alámbrica como: switches, Access point, Servidores, entre otros. Además, disponer de medios para realización y acceso a backups ya configurados.

7 CONCLUSIONES

Este desarrollo permitirá elaborar un documento escrito donde podremos identificar información conceptual y estado de arte, métodos, herramientas de diagnóstico y análisis de la red, los controles de seguridad más recomendados a aplicar para coadyuvar en el mejoramiento de la seguridad en una red de datos.

Así mismo se podrá encontrar el proceso de diagnóstico realizado mediante las herramientas identificadas para tal fin, con las pruebas recolectadas y las bases bajo las que se realizó la revisión, análisis e identificación del estado de seguridad actual de la red de datos en la Alcaldía de San Antero Córdoba.

En el documento se podrán identificar y encontrar definidos los controles y mecanismos de seguridad que deben ser aplicados para garantizar un ambiente controlado y recomendado según las buenas prácticas de TI, para la red de datos de la alcaldía de San Antero Córdoba.

Todo el desarrollo será organizado y presentado en documento monográfico, propuesta de solución documentada y soportada con la mejor opción para que sea implementada por parte de la entidad, en pro de la optimización de la seguridad en la red de datos, de la alcaldía de San Antero Córdoba.

Como resultado de todo lo anterior se pretende que la entidad posea un instrumento o herramienta guía para tener en cuenta y mejore sus procesos a través de la retroalimentación de conceptos y pruebas que se dejaran de base para crear conciencia de la importancia de invertir y asumir medidas que puedan subsanar las debilidades y potenciar a la entidad para cumplir con el logro de objetivos operativos y estratégicos en el área de TI y como consecuencia el área de gestión Estratégica. Lo cual proporcionará un mejoramiento desde todos los puntos de vista en la entidad, seguridad, desempeño, gestión, y logrará la iniciación en el desarrollo de

proyectos de TI, encaminados hacia el desarrollo del sistema de Gestión de Seguridad de la Información, que requiere la entidad.

8 DIVULGACIÓN

Este trabajo es un proyecto de carácter privado que interesa a la comunidad conformada por el recurso humano de la Alcaldía de San Antero Córdoba, quienes son los únicos interesados en saber y conocer el resultado del informe concluido, Para su divulgación se realizará invitaciones a los miembros directivos y de apoyo de la entidad, con el fin de que se familiaricen con el material y conozcan el resultado del estudio y sean conscientes de las recomendaciones, para lograr esto se aprovechara herramientas como la socialización, el correo electrónico, charlas con los diferentes niveles y roles en la entidad.

9 BIBLIOGRAFÍA

AXENCE, Herramienta de red, 2016. obtenida de http://axence.net/en/axence-nettools/

BORTNIK, Sebastián, Universidad Nacional Autónoma de México, Pruebas de Penetracion para principiantes- 5 Herramientas. Obtenido de http://revista.seguridad.unam.mx/numero-18/pruebas-de-penetraci%C3%B3n-para-principiantes-5-herramientas-para-empezar

CISCO, Soluciones De Control Y Contención De Amenazas, Publicaciones, Copyright © 2007 Cisco Systems, Inc. Obtenido de: http://www.cisco.com/c/dam/global/es_es/assets/publicaciones/07-08-cisco-control-contencion-amenazas.pdf

CRATON, Jhon, Home Blog Projects CV Contact, obtenido de https://joncraton.org/blog/46/netcat-for-windows/

EMC^2 RSA, Informe Técnico, Detección y Respuesta ante Amenazas basadas en Inteligencia, 2014, obtenido de https://colombia.emc.com/collateral/white-paper/h1304-intelligence-driven-threat-detection-response-wp.pdf

GESTIÓN DE RED, obtenido de https://eetac.upc.edu/ca/fitxers/Gestion_de_red.pdf

INSECURE.ORG, Las 75 herramientas de seguridad más usadas, obtenido de http://insecure.org/tools/tools-es.html

ITU, Unión Internacional de Comunicaciones, Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo, 2003. Obtenido de https://www.itu.int/rec/T-REC-X.805-200310-I/es

MIERES, Jorge, Ataques informáticos, 2009 https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

OFFENSIVE SECURITY, Kali Linux documentación Oficial, 2016. Obtenido de http://es.docs.kali.org/introduction-es/que-es-kali-linux

REPOSITORIO UNIVERSIDAD TECNOLÓGICA DE PEREIRA, Facultad de Ingenierías, Vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos de las organizaciones, 2009 obtenido de, http://repositorio.utp.edu.co/dspace/bitstream/11059/2734/1/0058R173.pdf

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, Facultad de Ingeniería, Fundamentos de Criptografía, 2016 http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/13-servicios-y-mecanismos-de-seguridad/132-mecanismos-de-seguridad

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, Facultad de Ingeniería, Fundamentos de Criptografía, 2016 http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/13-servicios-y-mecanismos-de-seguridad/131-servicios-de-seguridad

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, Facultad de Ingeniería, Fundamentos de Criptografía, 2016 http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/15-arquitectura-de-seguridad-de-osi/152-servicios-de-seguridad-de-osi

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, Facultad de Ingeniería, Fundamentos de Criptografía, 2016 http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/14-ataques/141-introduccion

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LA COMNICACION TIC DE COLOMBIA. Ley 1273 de 2009 de la protección de la información y de los datos. [Consultado 10 de Mayo de 2015]. Disponible en Internet: www.mintic.gov.co/portal/604/articles-3705_documento.pdf

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMNICACIONES TIC DE COLOMBIA. Ley 1341 de 2009 del marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones. [Consultado 10 de Mayo de 2015]. Disponible en Internet: www.mintic.gov.co/portal/604/articles-3707_documento.pdf

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMNICACIONES TIC DE COLOMBIA. Ley 1581 de 2012 para la protección de datos personales. [Consultado 10 de Mayo de 2015]. Disponible en Internet: http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

VERGARA, Kevin, Blog informático, 2016. 12 herramientas de diagnóstico y monitoreo de red, http://www.bloginformatico.com/12-herramientas-de-diagonstico-y-monitoreo-de-redes-axence-nettools.php

WIKIPEDIA, Seguridad Informática, 2016, obtenido de https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

WIKIPEDIA, Snort, 2016. obtenido de https://es.wikipedia.org/wiki/Snort

WIKIPEDIA, Wireshark, 2016, obtenido de https://es.wikipedia.org/wiki/Wireshark

Michel Miranda Cairo, Osmany Valdés Puga, Iván Pérez Mallea, Renier Portelles Cobas, Raúl Sánchez Zequeira, UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS. La Habana, Cuba. {mcairo, ovaldes, imallea, renierpc, raulsz}@uci.cu, Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática, Revista Cubana de Ciencias Informáticas (2014-2016). https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=987&path%5B%5D=416

MARTÍNEZ MOLINA, Kelly Johanna y PACHECO MENESES, Javys y ZÚÑIGA SILGADO, Isaac, (2009), Firewall – Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas y Medianas Empresas), http://revistas.uis.edu.co/index.php/revistauisingenierias/article/view/506/830

FRANCO, David A. y PEREA, Jorge L. y PUELLO, Plinio, Universidad de Cartagena, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática, GIMATICA, Metodología para la Detección de Vulnerabilidades en Redes de Datos, (2011), http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=1ee99cfe-aa41-4ec9-9096-79bd205072e0%40sessionmgr4008&vid=1&hid=4207

SGS Colombia S.A., División S&SC, VISIÓN GENERAL ISO 27001:2013. (2015).

OWASP ZAP Zed Attack Proxy Project [en línea]. [Consultado el 7 de Octubre de 2016]. Disponible en: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

ANEXOS

Anexo A Propuesta de Solución

Las recomendaciones de solución están orientadas a un trabajo que la Alcaldía de San Antero debe realizar en dos ejes principales el eje administrativo y de planeación estratégica y el eje Tecnológico.

De acuerdo con las diversas pruebas realizadas y al análisis que se realizó de las mismas se puedo encontrar que los sistemas informáticos son relativamente estables y aceptables, hay manejo de software legal en sus equipos, lo que permite que siempre se tenga acceso a las actualizaciones de los mismos. Los equipos que manejan las actividades críticas tienen condiciones básicas mínimas de seguridad como son antivirus con licencias pagadas y algunos con licencias gratuitas, lo que agrega a nivel lógico una protección sumado a la protección que ofrece el sistema de cableado que minimiza la facilidad de acceder a intrusos a la red por parte de robos de señal o canal inalámbrico. Estas son fortalezas pequeñas que se pueden maximizar con un buen plan administrativo y un buen agregado tecnológico de dispositivos que generen un esquema de red mejorado.

Por lo anterior y según las buenas prácticas de TI y enfocados en los controles recomendados en la norma ISO 27001:2013 se detecta la necesidad de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), el cual es fundamental debido a que se apoya en el ciclo (PHVA) Planificar, Hacer, Verificar y Actuar, lo que le dará a la entidad unas medidas y formas de proceder que al ser implementadas aunaran esquemas de control que actualmente no existen en la Alcaldía de San antero.

La implementación de un SGSI permitirá hacer una identificación más puntual y detallada que organice e identifique los procesos y procedimientos de las áreas críticas y definirá mecanismos de control y políticas de seguridad de la información, así como el desarrollo integral del recurso humano como elemento importante y

vulnerable en el esquema de seguridad de la entidad, y así la Alcaldía de San Antero podrá crear un proceso integrado de conocimiento y cultura de seguridad hasta el punto que el actor interno respete las políticas, procedimientos y aspectos de seguridad definidos y recomendados, hasta convertirlo en un hábito de desempeño institucional. Todo esto deberá ser apoyado y aprobado por la Alta dirección en este caso La cabeza más visible el alcalde mayor con un compromiso delegado hacía todos y cada uno de los integrantes del cuerpo laboral en la entidad en todos los niveles.

La recomendación principal para este ente territorial es que se apoye en la Norma Técnica NTC-ISO-IEC colombiana 20071 la cual es una adopción idéntica por traducción de la norma ISO/IEC 27001:2013. O en su defecto implemente dicha norma sin excluir ningún requisito especificado de los numerales 4 al 10, de la misma.
Esta norma establece que la Alcaldía de San Antero deberá realizar una serie de identificaciones y análisis de sus procesos, para ello deberá:

4. Contexto de la Organización.
Analizar el Contexto de la Organización La alcaldía de San Antero debe determinar los factores externos y externos que pueden afectar su capacidad de logro de resultados el proceso de Gestión de Seguridad de la información.

5. Liderazgo.
Identificar el Líder del proceso La alta dirección en este caso el alcalde, deberá demostrar el compromiso y su liderazgo en el proceso de Gestión de Seguridad de la información. Para ello debe

establecer y aprobar la política, los roles y responsabilidades y autoridades en la entidad.

6. Planificación.
Realizar una planificación Aquí la entidad definir una planeación y valoración de las acciones para el tratamiento de los riesgos y oportunidades de los objetivos de seguridad.

7. Soporte.
Definir un Soporte La Alcaldía de San Antero deberá determinar y proporcionar los recursos (económicos y humanos) necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI. Donde debe haber definida una competencia, creación de conciencia, comunicación, y documentación que soporte el proceso.

8. Operación.
Hacer una puesta en operación Es la fase donde debe iniciar la implementación de todo lo definido en las fases anteriores, apoyado en planificación para cumplir los requisitos definidos.

9. Evaluación del Desempeño.
Realizar evaluación del desempeño Deberá hacer el seguimiento y evaluar la eficacia del SGSI.
Realizar auditoria Interna Deberá realizar verificaciones de la operación y cumplimiento y conveniencia y eficacia del SGSI.

10. Mejora.
Realizar mejora continua Deberá identificar conformidades y no conformidades del sistema para realizar los cambios respectivos e ir mejorando continuamente.

Todo lo anterior deberá ser logrado con un grupo interdisciplinario conformado por las diferentes dependencias y asesores que considere la Alta dirección de la Alcaldía de San Antero que deben intervenir en el proceso. Y así mismo la Norma aplica una serie de controles que deben ser cumplidos para poder implementarla, en lo cual engloba y enfoca todos y cada uno de los aspectos mencionados en las fases nombradas anteriormente.

Es por ello por lo que la Alcaldía deberá cumplir con los objetivos de control y controles definidos en el anexo A de la norma al implementar el SGSI basado en ISO27001:2013, los cuales se identifican a continuación:

Tabla 8 Controles ISO27001

A.5.	Política de la seguridad de la información
A.6.	Organización de la seguridad de la información
A.7.	Seguridad de los recursos humanos.
A.8.	Gestión de activos.
A.9.	Control de acceso.
A.10.	Criptografía
A.11.	Seguridad física y ambiental
A.12.	Seguridad de las operaciones.
A.13.	Seguridad de las comunicaciones.
A.14.	Adquisición, desarrollo y mantenimiento de sistemas.
A.15.	Relaciones con los proveedores.
A.16.	Gestión de incidentes de seguridad de la información.

A.17.	Aspectos de seguridad de la información de la gestión de la continuidad de negocio.
A.18.	Cumplimiento.

Este es un proceso apoyado en estándares que buscan el mejoramiento y la aplicación de buenas Prácticas de TI como el resultado de acciones ya probadas en organizaciones que han sacado el mejor provecho al tomarlos en referencia y aplicarlos, por esta razón se recomienda esta solución como apoyo para el mejoramiento y control a los procesos y procedimientos en la Alcaldía de San Antero en su proceso y responsabilidad de Salvaguardar la información que el ente territorial genera y maneja como requisito legal que debe cumplir.

En Cuanto al Hardware, todo el Sistema detallado anteriormente deberá asimismo ser apoyado con herramientas tecnológicas que trabajen en pro de los aspectos de seguridad y privacidad de la información, es necesario implementar seguridad perimetral con el fin de contrarrestar el acceso de actores no autorizados mediante dispositivos activos en la red, como firewalls, UTMS, proxys, sistemas de detección de intrusos, definir un esquema de servicios manejado mediante el uso de servidores configurados y preparados específicamente para el manejos de temas específicos como el servicio de archivos, el servicios de correo electrónico, el servicio de impresión, el servicio de Backups, servicios de control de acceso, entre otros..

En Cuanto a Tecnología, así mismo se sugiere la segmentación de red para que se distribuya seguridad de acuerdo con la criticidad de la información que manejen las áreas, por lo cual se crearían segmentos de red por áreas de trabajo limitando los accesos y regulando el tráfico interno entre áreas y recursos críticos que maneja la entidad. Esta medida puede proporcionará mejor uso al ancho de banda y aumento en los tiempos de respuesta en los sistemas de información internos que brindan

servicios con necesidad de tiempos de respuestas óptimos para la realización de transacciones locales.

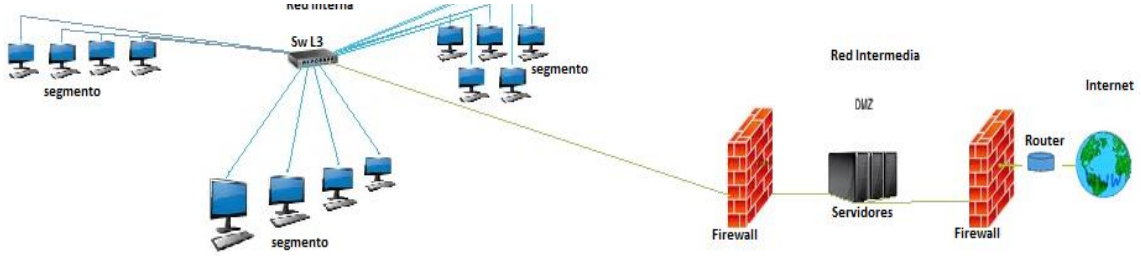
Se recomienda incluir en la capacidad tecnológica un sistema espejo para los servicios de información críticos (que incluya hardware y software) como mínimo para garantizar la continuidad del servicio con tiempos de respuesta aceptables en caso de un incidente u ocurrencia de un riesgo, lo cual es fundamental para mantener la credibilidad en la entidad.

Así mismo se recomienda adquirir e implementar un sistema de gestión de red que permita tener el control local y remoto de los distintos dispositivos en la red de datos y poder hacer un continuo monitoreo y control de la misma.

Las anteriores soluciones tecnologías estarían apoyadas en hardware y software que permita y de la capacidad a la Alcaldía de San Antero de Administrar y dar gestión a cualquier necesidad que requiera controlar en materia de tráfico y manejo de flujo de información en la red de datos de la entidad.

El esquema de red y los mecanismos de seguridad recomendados para la Alcaldía de San Antero, es el siguiente:

Imagen 17 Esquema de Red recomendado para la Alcaldía de San Antero Córdoba.



Fuente: Autores

El esquema referenciado en la figura anterior consta de dos firewalls que definirán y serán la frontera para la definición de la DMZ donde estarán ubicados los servidores, que darán servicio tanto a usuarios internos y externos, pero de acuerdo a las reglas definidas para el acceso. Una red interna segmentada para optimizar el flujo de datos y aprovechar el ancho de banda del canal, mediante configuración de switchs capa 3 que permitirán administrar y asignar control al flujo por puertos. Una red externa que tendrá acceso de acuerdo con los servicios autorizados y controlados mediante los firewalls y el enrutador.

Se recomienda adquirir un software para la administración y gestión de los dispositivos activos de la red, con el fin de que el administrador designado pueda desde un punto observar los movimientos y acciones que las estaciones están realizando y pueda tomar las medidas correctivas por medio de controles automáticos o políticas que se evalúen en el caso de la ocurrencia de un incidente que se salga de los parámetros definidos.

El entorno de Red como se detalla en el esquema de la misma deberá ser descrito y documentado en su configuración de hardware de comunicaciones y software en uso y adicionado, los controles establecidos a la red, estado general de los computadores, gestores de bases de datos con aplicaciones críticas y aspectos relativos a la seguridad de la red.

La configuración de los servidores deberá quedar explícito en la documentación las características de configuración, sistema operativo, software las particiones, entornos (pruebas y real), bibliotecas de programas entre otros.

El Entorno de aplicaciones identificar los procesos de transacciones, sistemas de gestión de base de datos.

Los productos y herramientas se deberán Identificar el software de programación, software de gestión de bibliotecas y para operaciones automáticas.

Seguridad de los servidores: la entidad deberá realizar la identificación y verificación de los usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, entre otros.

La gestión de sistema de información deberá verificar con los proveedores que estos cumplan con las normas legales y de seguridad para el manejo de las transacciones.

La administración de sistemas deberá quedar especificado y asignado los controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.

La Seguridad se debe verificar la existencia de controles que garanticen la integridad del sistema, confidencialidad autenticidad y disponibilidad.

La gestión del cambio se deberá implementar en la medida de lo necesario y posibilidad presupuestal armar o separar un entorno virtual o físico para la realización de pruebas y la producción a nivel del software y los controles de procedimientos para la migración de programas software aprobado y probado.

Como la alcaldía de San antero Carece de ciertos elementos dentro de su esquema de red actual, para mejorar y agregar control fue diseñado y recomendado el esquema de la Fig. 1, el cual queda a disposición del ente territorial para que sea implementado de acuerdo con su presupuesto e intenciones de ejecución de la propuesta de solución recomendada.

Software, Equipos y dispositivos recomendados

Tabla 9 Equipos y dispositivos

Equipo Servidor	Intel® Xeon® E5-2630 v4 de 2,2 GHz; memoria caché de 25 M; 8 GT/s QPI; Turbo; HT; 8 C/16 T (85 W); mem. máx. de 2133 MHz	
	Intel® Xeon® E5-2630 v4 de 2,2 GHz; memoria caché de 25 M; 8 GT/s QPI; Turbo; HT; 8 C/16 T (85 W); mem. máx. de 2133 MHz	

	RDIMM de 8 GB, 2400 MT/s, clasificación simple, ancho de datos x8	
	Disco duro de conexión en marcha de 300 GB a 15.000 RPM SAS de 12 Gb/s y 2,5", 3,5" EN PORTADORA HÍBRIDA	
	Windows Server® 2016, Standard, 16 NÚCLEOS	
	Windows Server® 2016, Standard, 16 NÚCLEOS, kit de medios	
	Windows Server® 2016, Standard Ed, licencia adic., 2 NÚCLEOS	
	Pack de 5 CAL de USUARIO de Windows® Server 2016	
Equipo Proxy	**Implementado en Linux**	**$ 0.**
Firewall Cisco	**ASA5512-K9**	**5.790.000**
	Sesiones simultáneas 100.000	
	Sesiones de usuario VPN sin cliente o AnyConnect 250	
	VLAN 50 / 100	
Switch	D-Link DGS-1510-52X switch capa 3 48 ports	**3.043.656**
Monitor de Red	PRTG Network Monitor X500	**4.800.000**
Monitor de red	Software libre	**$0.**

Fuente: Autores

EL SGSI y la adquisición de tecnología lograrán que se incluyan controles que pueden ser principalmente de dos tipos manuales o automáticos.

El control Manual se realizaría sin utilizar herramientas computacionales y sería ejecutado por usuarios o personal del área de informática o en su efecto un personal autorizado.

El control automático se realizaría por medio de las herramientas automatizadas que se recomiendan para hacer gestión, seguimiento, aplicación, comunicación y operación con el apoyo de programas o software programable en los dispositivos activos configurables.

La entidad así podrá tener Controles Preventivos, que le permitirán establecer medidas y acciones que evitarán la ocurrencia de incidentes que afecten negativamente los objetivos de la alcaldía de San antero. Y los Controles Detectivos, para tener el control sobre la ocurrencia de un hecho y permitir activar las alarmas en el sistema de forma que pueda hacerse una gestión o aplicar el plan de contingencia al descubrirse el incidente.

Para lograr todos estos objetivos la entidad debe tener en cuenta unos elementos que trabajan sobre el área de TI, así:

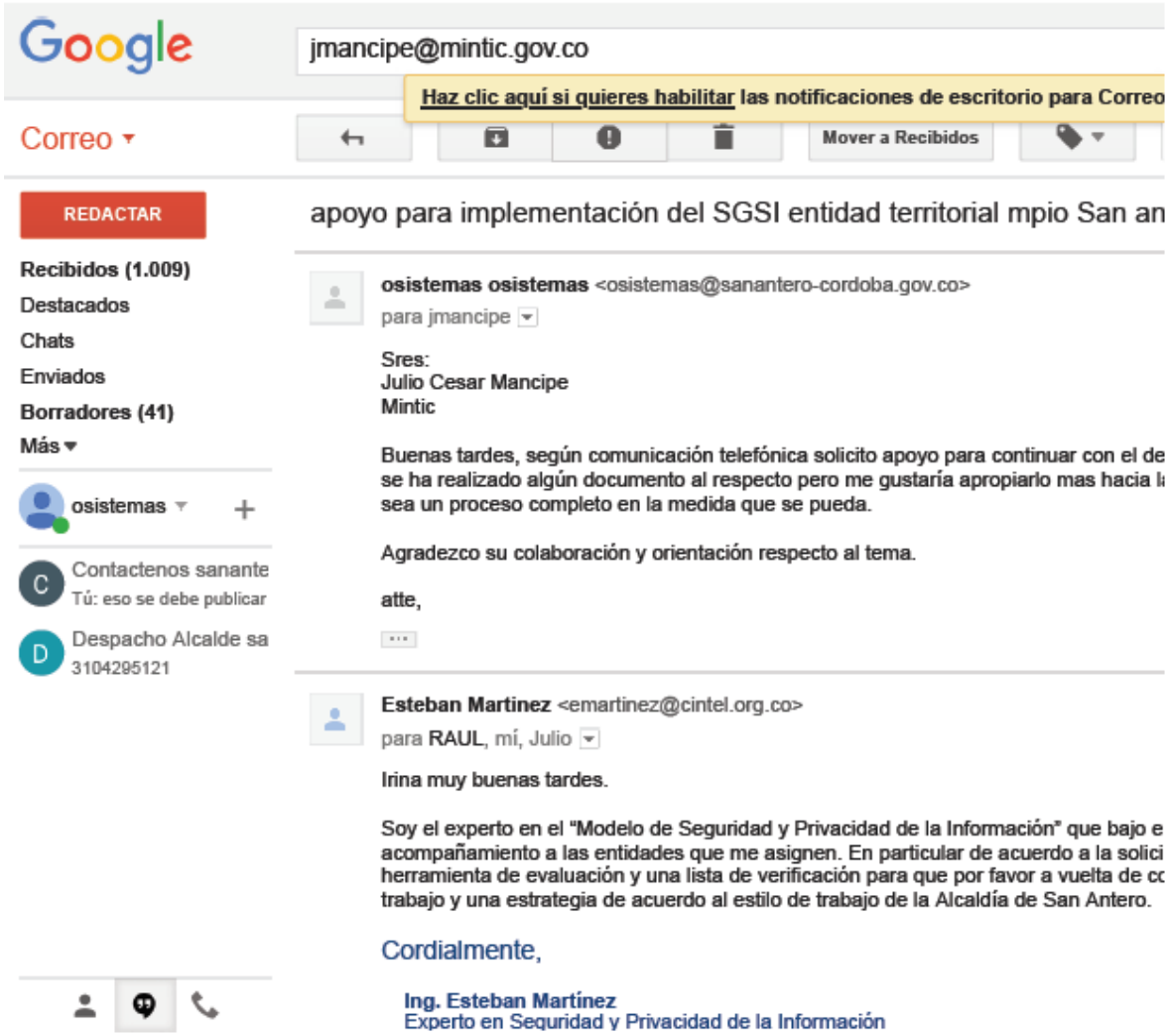
La Alcaldía de San antero para implementar el sistema de Gestión de Seguridad de la Información SGSI debe:
Adoptar y seguir una metodología única para el desarrollo de proyectos, con el fin de unificar las actividades de análisis y diseño de los sistemas.
Adoptar una buena planeación programación y presupuesto para el desarrollo del sistema.
Contar con la participación de usuarios para garantizar un buen desarrollo y concienciación del sistema.
Contratar a personal con el conocimiento experiencia y capacidad para el desarrollo y configuración de sistemas informáticos.

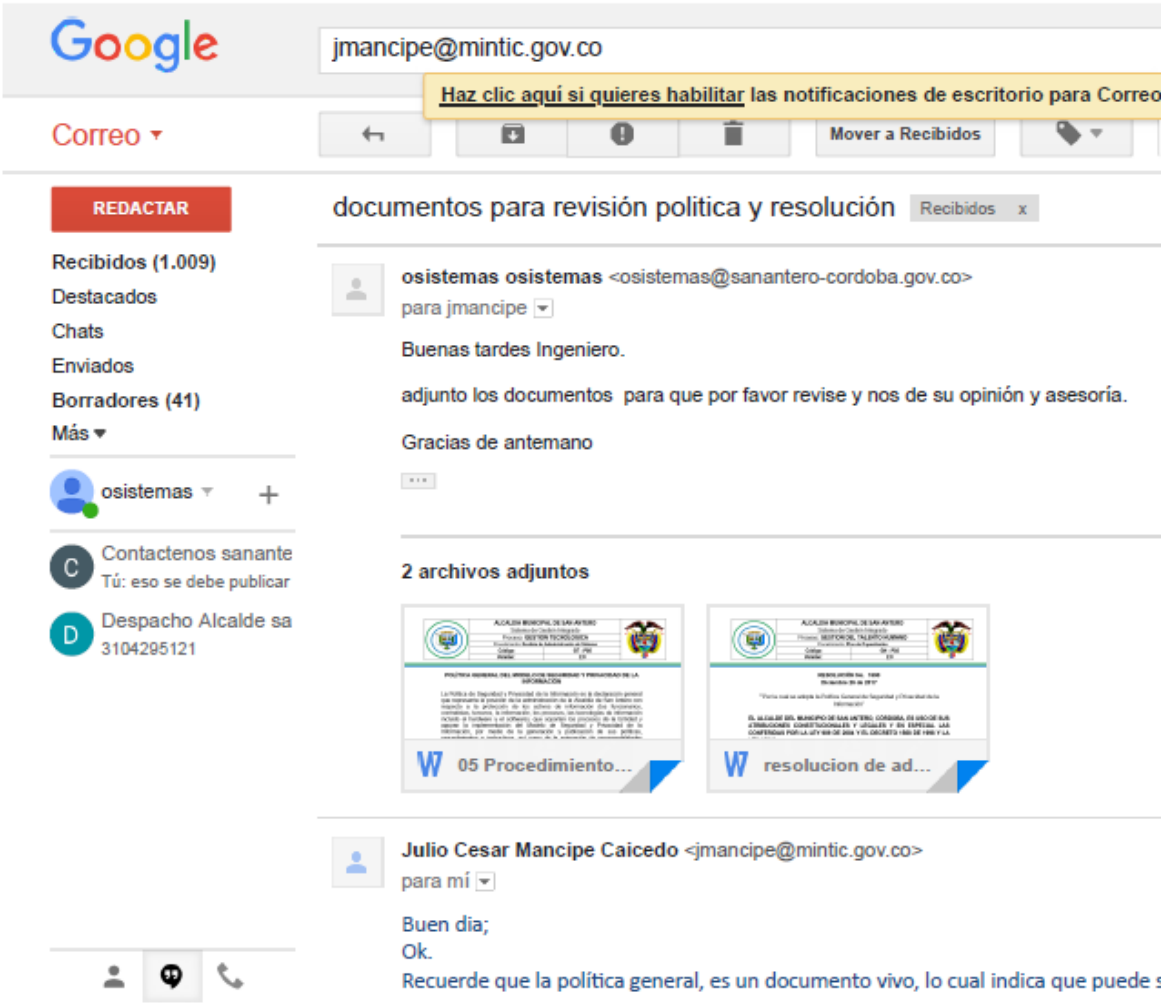
Utilizar requerimientos técnicos (hardware, software y personal) para el desarrollo e implementación.
Diseñar y aplicar las pruebas previas a la implementación.
Supervisar permanentemente el avance de actividades
Todos los procesos y procedimiento deben estar soportados y documentados manuales de usuario, de operación, manual técnico de los sistemas, Manual de seguimiento y control, Manuales de mantenimiento, Manuales de Configuración y seguridad.

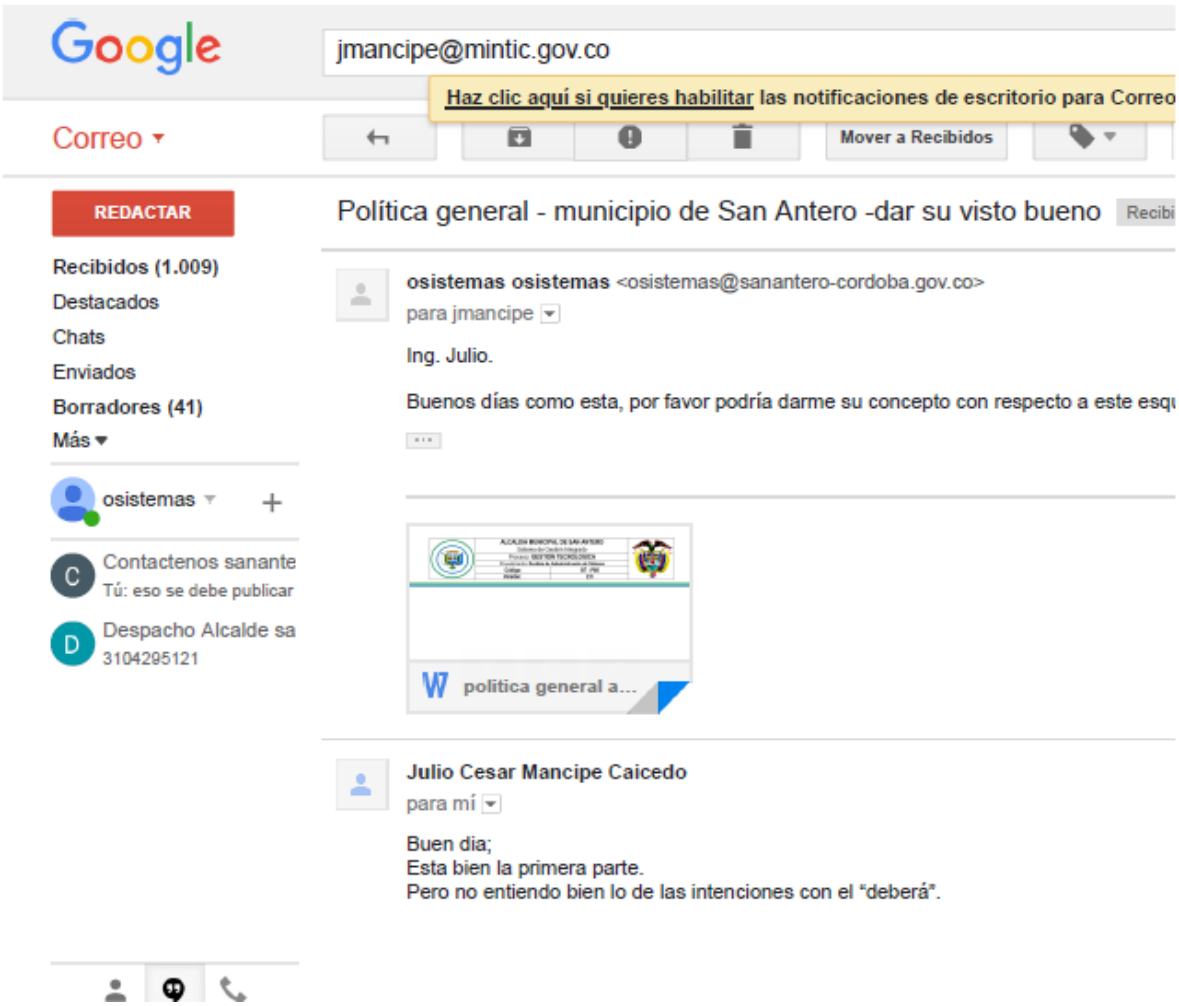
Si la Alcaldía de San Antero logra ejecutar e implementar esta propuesta de solución de acuerdo con el orden y a la responsabilidad que deberá asumir para desarrollar el proceso, con todos estos elementos detallados y conocidos se podrá decir que tendrá así la entidad un conocimiento sobre la estructura de seguridad de TI en la organización.

Anexo B Comunicación ministerio de las TIC

Anexamos la comunicación permanente con el ministerio de las TIC para el desarrollo de las actividades realizadas en este proyecto debido a que la alcaldía de San Antero al ser una entidad pública debe tener el acompañamiento del ministerio. Esto afectó los tiempos de entrega del proyecto debido a que la comunicación no era tan fluida como se esperaba.


Google
jmancipe@mintic.gov.co
Haz clic aquí si quieres habilitar las notificaciones de escritorio para Correo
Correo
Mover a Recibidos
REDACTAR
Recibidos (1.009)
Destacados
Chats
Enviados
Borradores (41)
Más
osistemas
Contactenos sanante
Tú: eso se debe publicar
Despacho Alcalde sa
3104295121
apoyo para implementación del SGSI entidad territorial mpio San an
osistemas osistemas <osistemas@sanantero-cordoba.gov.co>
para jmancipe
Sres:
Julio Cesar Mancipe
Mintic
Buenas tardes, según comunicación telefónica solicito apoyo para continuar con el de
se ha realizado algún documento al respecto pero me gustaría apropiarlo mas hacia l
sea un proceso completo en la medida que se pueda.
Agradezco su colaboración y orientación respecto al tema.
atte,
Esteban Martinez <emartinez@cintel.org.co>
para RAUL, mí, Julio
Irina muy buenas tardes.
Soy el experto en el "Modelo de Seguridad y Privacidad de la Información" que bajo e
acompañamiento a las entidades que me asignen. En particular de acuerdo a la solici
herramienta de evaluación y una lista de verificación para que por favor a vuelta de cc
trabajo y una estrategia de acuerdo al estilo de trabajo de la Alcaldía de San Antero.
Cordialmente,
Ing. Esteban Martínez
Experto en Seguridad y Privacidad de la Información


Google
jmancipe@mintic.gov.co
Haz clic aquí si quieres habilitar las notificaciones de escritorio para Correo
Correo
Mover a Recibidos
REDACTAR
Recibidos (1.009)
Destacados
Chats
Enviados
Borradores (41)
Más
osistemas
Contactenos sanante
Tú: eso se debe publicar
Despacho Alcalde sa
3104295121
documentos para revisión politica y resolución
Recibidos x
osistemas osistemas <osistemas@sanantero-cordoba.gov.co>
para jmancipe
Buenas tardes Ingeniero.
adjunto los documentos para que por favor revise y nos de su opinión y asesoría.
Gracias de antemano
2 archivos adjuntos
05 Procedimiento...
resolucion de ad...
Julio Cesar Mancipe Caicedo <jmancipe@mintic.gov.co>
para mí
Buen dia;
Ok.
Recuerde que la política general, es un documento vivo, lo cual indica que puede s


Google
jmancipe@mintic.gov.co
Haz clic aquí si quieres habilitar las notificaciones de escritorio para Correo
Correo
Mover a Recibidos
REDACTAR
Recibidos (1.009)
Destacados
Chats
Enviados
Borradores (41)
Más
osistemas
Contactenos sanante
Tú: eso se debe publicar
Despacho Alcalde sa
3104295121
Política general - municipio de San Antero -dar su visto bueno
Recibi
osistemas osistemas <osistemas@sanantero-cordoba.gov.co>
para jmancipe
Ing. Julio.
Buenos días como esta, por favor podría darme su concepto con respecto a este esqu
politica general a...
Julio Cesar Mancipe Caicedo
para mí
Buen dia;
Esta bien la primera parte.
Pero no entiendo bien lo de las intenciones con el "deberá".

Anexo C Resolución donde se adopta la política general de seguridad informática

RESOLUCIÓN No. 1590
Diciembre 26 de 2017

""Por la cual se adopta la Política General de Seguridad y Privacidad de la Información"

EL ALCALDE DEL MUNICIPIO DE SAN ANTERO, CÓRDOBA, ES USO DE SUS ATRIBUCIONES CONSTITUCIONALES Y LEGALES Y EN ESPECIAL LAS CONFERIDAS POR LA LEY 909 DE 2004 Y EL DECRETO 1568 DE 1998 Y LA LEY 136 Y

CONSIDERANDO:

1. Que la Ley 1341 de 2009, estableció el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, incorporando principios, conceptos y competencias sobre su organización y desarrollo e igualmente señaló que las Tecnologías de la Información y las Comunicaciones deben servir al interés general y, por tanto, es deber del Estado promover su acceso eficiente y en igualdad de oportunidades a todos los habitantes del territorio nacional.

2. Que el numeral 8 del artículo segundo de la citada Ley establece que con el fin de lograr la prestación de servicios eficientes a los ciudadanos, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones en el desarrollo de sus funciones.

3. Que el Decreto 1083 de 2015, adicionado por el Decreto 415 de 2016, establece la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones, cuyo ámbito de aplicación, de acuerdo con el artículo 2.2.35.2, corresponde a las entidades del Estado de orden nacional y territorial, los organismos autónomos y de control.

4. Que el artículo 2.2.35.3 del Decreto 1083 de 2015, adicionado por el Decreto 415 de 2016, establece como objetivos del fortalecimiento institucional: "3. *Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la*

gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones TIC. Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia" y "11. *Desarrollar estrategias de gestión de información para garantizar la pertinencia, calidad, oportunidad, seguridad e intercambio con el fin de lograr un flujo eficiente de información disponible para el uso en la gestión y la toma de decisiones en la entidad y/o sector*".

5. Que mediante el Decreto 2573 de 2014, "*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea*", se describen los lineamientos, se incorporan mejores prácticas y se orienta la implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información y se reglamenta el Marco de Referencia de Arquitectura Empresarial para Entidades del Estado, el cual es un modelo de referencia puesto a disposición del Estado Colombiano para servir como orientador estratégico de las arquitecturas empresariales, lo cual debe estar articulado con los lineamientos de seguridad de la información.

6. Que el Artículo 2.2.9.1.2,1 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015, establece como cuarto componente, para desarrollar los fundamentos de la estrategia que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea, el de la Seguridad y privacidad de la Información.

En mérito de lo anterior, esta alcaldía,

RESUELVE:

ARTICULO PRIMERO. Adóptese la Política General de Seguridad y Privacidad de la Información, en la Alcaldía de San Antero, Córdoba, como norma fundamental para el desarrollo de proyectos de tecnología con una gestión eficiente y optimización de los recursos, servicios TIC, y los sistemas de información.

ARTÍCULO 2º. Las políticas aplicaran a los servidores públicos, contratistas, proveedores y/o terceros usuarios de la información impresa, digital, y la soportada sobre las tecnologías de información y las comunicaciones de la Alcaldía de San Antero, Córdoba.

ARTÍCULO 3º. Acójase lo dispuesto en el numeral **5.2 de la Norma ISO/IEC 27001:2013. Y en el** numeral A.5, Anexo A de la misma Norma.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dado en San Antero a los (26) días del mes de diciembre de 2017

DENNYS CHICA FUENTES
Alcalde Municipal

Anexo D Política general del modelo de seguridad y privacidad de la información

POLÍTICA GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Introducción

La entidad territorial ha tenido un crecimiento ascendente, que consiste en la adición de dispositivos, herramientas informáticas y sistemas de información con el fin de producir y ser más eficientes en el desempeño y tratamiento de los datos que recibe y genera. Orientando todo a los servicios de información y la atención al ciudadano, buscando el mejoramiento continuo.

Esta tendencia coloca a la información como el activo más importante en la entidad, por ello debe ser protegido bajo los principios básicos de la seguridad de la misma, como es su disponibilidad, integridad y confidencialidad, razón por la cual se está trabajando en el mejoramiento de los procesos y los procedimientos tecnológicos.

En este sentido La alcaldía de San Antero ha definido La Política General de Seguridad y Privacidad de la Información como un lineamiento base para apoyar una serie de políticas adicionales y mecanismos que debe adoptar para poder cumplir con este objetivo, y que representará la posición de la administración de la Alcaldía de San Antero con respecto a la protección de los activos de información (funcionarios, contratistas, terceros, información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y serán una parte básica en la implementación del Modelo de Seguridad y Privacidad de la Información, donde se generaran y publicarán políticas específicas, procedimientos e instructivos, asignaran responsabilidades generales y específicas para la gestión de la seguridad de la información. Esta política se basa fundamentalmente en el estándar de la norma técnica colombiana NTC-ISO-27001:2013.

La alcaldía de San Antero para asegurar la dirección estratégica de la Entidad, se trabajar por la seguridad, la gestión de la información, la adquisición de tecnología y sistemas de información, facilitar el acceso y uso de las mismas a los usuarios, cuidando y asegurando el cumplimiento, actualización de políticas y estándares de TI. Esto estableciendo una compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- ✓ Minimizar el riesgo de los procesos misionales de la entidad, trabajando en el cumplimiento de los principios de seguridad de la información y la función administrativa.
- ✓ Mantener la confianza de los funcionarios, contratistas y terceros, mediante la definición de políticas, procedimientos e instructivos en materia de seguridad de la información que agreguen protección a los activos de información.
- ✓ Mantener la gestión y el apoyo a la innovación tecnológica, buscando fortalecer la cultura de seguridad de la información en los funcionarios, terceros, practicantes y clientes de la Alcaldía de San Antero córdoba.
- ✓ Implementar el sistema de gestión de seguridad de la información de manera coherente definiendo reglas, responsabilidades, recursos, riesgos y periodos de seguimiento o actualización.
- ✓ Definir mecanismos para garantizar la continuidad del negocio frente a incidentes que pueden presentarse.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la Alcaldía de San Antero y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

Anexo E Manual de políticas de la información

MANUAL DE POLITICAS DE LA INFORMACIÓN

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Tabla de contenido

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

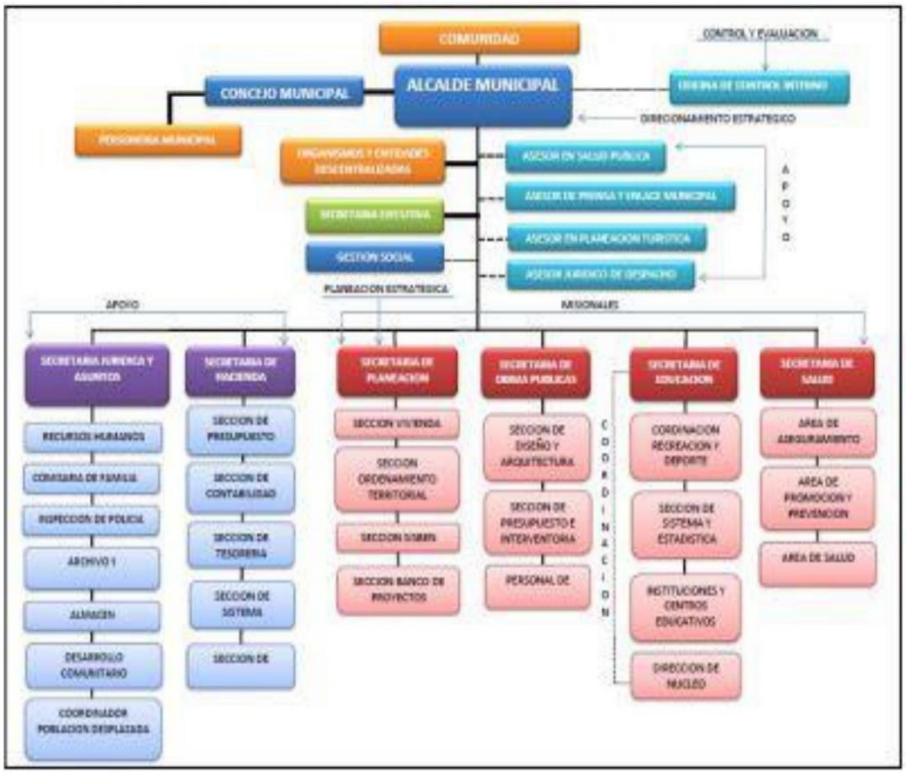
INTRODUCCIÓN

Este documento contiene las políticas definidas en el marco del sistema de Gestión de Seguridad de la información, y de acuerdo con los requisitos exigidos por el MPSI con el fin de dar seguridad en el manejo de la información en la realización de las diferentes actividades en la alcaldía de San Antero-Córdoba.

De manera que quede establecido y documentado las actividades que se deben realizar para el cumplimiento de los objetivos de este manual de políticas de seguridad de la Información.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

ORGANIZACIÓN



Fuente: Manual de Funciones y procedimientos Alcaldia de San antero

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

OBJETIVO

Definir directrices que permitan a la Alcaldía de San antero realizar acciones de manera más responsable y consciente a la hora de hacer manejo de la seguridad de la información en la entidad y así direccionarla al cumplimiento de los requisitos exigidos por el MSPI, hacía la implementación de un SGSI.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

ALCANCE

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la Alcaldía de San Antero y ciudadanía en general. Serán aplicadas a todos los procesos Misionales, de Apoyo y transversales, por ello serán socializadas y divulgadas en todos los medios de comunicación disponibles en el ente territorial.

SANCIONES

El incumplimiento a las políticas de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

1. TERMINOS Y DEFINICIONES

- ✓ **Mantenimiento Preventivo:** son una serie de actividades que se realizan de anticipadamente para prevenir la aparición de daños graves en los equipos electrónicos (computadores).

- ✓ **Red:** Conjunto de computadores y software interconectados por medio de dispositivos y medios físicos (hardware como servidores, tarjetas de red, cables, switches, routers) que intercambian impulsos eléctricos y permiten transmitir datos y compartir recursos entre sí.

- ✓ **Servidor:** Computador con características específicas y distintivas en software que brinda servicios a otros computadores, bajo el sistema cliente/servidor.

- ✓ **Copias de Seguridad:** Denominado Backup o respaldo, es una copia de archivos o datos originales que se hace para que estén disponibles en un medio de almacenamiento diferente, en caso de producirse una falla o pérdida de los almacenados en los equipos de cómputo en uso.

- ✓ **Administrador del sistema:** Persona encargada de llevar el control, gestionar, conceder permisos de toda una Red de ordenadores o un sistema informático.

- ✓ **Soporte:** Servicio o ayuda que se presta a los usuarios de la sala de informática de la I.E. el Rosario para resolver inconvenientes técnicos o relacionados con el área.

- ✓ **Usuario:** Persona que tiene acceso a la sala de informática y hace uso de los elementos y recursos informáticos.

- ✓ **Programas o aplicativos:** Conjunto de instrucciones estructuradas y ordenadas escritos en un lenguaje entendido por la máquina que permite ejecutar y realizar tareas de acuerdo al procedimiento definido en ellos.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

- ✓ **Hardware:** Elementos físicos que conforman una computadora o un sistema de informático.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

2. POLÍTICAS Y CONTROLES DE LA SEGURIDAD DE LA INFORMACIÓN

2.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1.1. Política General de la Seguridad de la Información.

Ver anexo N°. XX, especifica la política general y la resolución de adopción de la misma.

2.1.2. Política para Orientación de la Dirección en la Gestión de la Seguridad de la Información.

Objetivo.

Apoyar por parte de la Alta dirección con los recursos disponibles y un equipo de trabajo designado para cubrir las necesidades y cumplir los requisitos exigidos por el MPSI en la implementación de las políticas de seguridad de la información, dentro del marco de las leyes y reglamentos que regulan la acción administrativa de la entidad.

Aplicabilidad.

Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesor del ente territorial.

Directrices:

Incluir al Tema del Sistema de Seguridad de la información como eje principal al nivel de los temas misionales del ente territorial.

Definir un Rubro en el presupuesto anual para el apoyo y ejecución de acciones y proyectos encaminados a la implementación de Seguridad de la Información y gestión de la misma.

Crear Espacio de trabajo para revisar y evaluar las acciones tomadas para el cumplimiento de esta política de manera periódica.

Responsables:

Alta dirección, funcionarios del nivel Directivo y asesor del ente territorial.

2.1.3. Política para la Seguridad de la Información

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Objetivo.
Definir los lineamientos para garantizar la seguridad de la información, los cuales están avalados, aprobados por la Alta Dirección y divulgados a todos los actores que interactúan con el ente territorial.

Aplicabilidad.
Esta política aplica a la Alta dirección, funcionarios del nivel Directivo, Asesores y Área de Tecnología del ente Territorial.

Directrices:

Valorar los lineamientos definidos y adoptarlos como mecanismos para el cumplimiento de la política de seguridad de la información.

Responsables:
Alta dirección, funcionarios del nivel Directivo, asesor y Área de Tecnología del ente territorial.

2.2. Organización De La Seguridad De La Información

2.2.1. Política para Definición de la Organización Interna

Objetivo.
Definir como marco de referencia para la gestión e implementación de la seguridad de la información en el ente territorial a la norma ISO27001:2013, como eje para establecer, implementar, mantener y mejorar continuamente el MSPI y trabajar hacia un SGSI.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas del ente territorial.

Directrices:
Aplicar los Dominios correspondientes para cumplir los requisitos del MSPI y trabajar por la implementación del SGSI.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Responsables:
Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas del ente territorial.

2.2.1.1. Política para Asignación de Roles y Responsabilidades de la seguridad de la Información.

Objetivo.
Definir los responsables de la seguridad de la Información y los roles que cumplirán dentro del esquema en el MSPI, para la operación, gestión y administración de la seguridad de la información en la Alcaldía de San antero.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, de la Alcaldía de San antero.

Directrices:
Designar al recurso humano requerido y necesario para cumplir con los requisitos exigidos para trabajar por la implementación del SGSI en el MSPI.

Establecer de acuerdo con la estructura de la Alcaldía de San Antero, el comité de Seguridad de la Información o quien haga sus veces, asignando roles y responsabilidades a los miembros.

Definir la regularidad de las capacitaciones en seguridad de la información y la asistencia a las mismas por parte de los responsables de la administración y operación de la seguridad de los sistemas de información en la Alcaldía de San antero.

Conocer el contacto y/o autoridades responsables para el reporte de incidentes en caso de ser necesario y designar el o los funcionarios responsables de hacer ese contacto y apoyar el manejo del incidente y el plan de contingencia.

Incluir los requisitos de seguridad exigidos por la norma en cada dominio dentro de la planeación y desarrollo de cualquier proyecto ejecutado en la Alcaldía de San Antero.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Definir los roles, funciones y responsabilidades de operación y administración a los funcionarios encargados de los sistemas de Información de la Alcaldía de San Antero.

Documentar de manera tacita cada uno de los roles, funciones y responsabilidades de operación y administración definidos y asignados a los funcionarios encargados de los sistemas de la Información de la Alcaldía de San Antero.

Responsables:
Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas del ente territorial de la alcaldía de San antero.

.

2.2.2. Política para Uso de Dispositivos Móviles

Objetivo.
Definir los lineamientos para el uso y tenencia de dispositivos móviles (portátiles, tabletas, Smart phones) asignados por la Alcaldía de San Antero para trabajo en campo o cualquier área diferente al puesto de trabajo.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, entes de control del ente territorial.

Directrices:
Las herramientas como dispositivos móviles serán usadas por los usuarios asignados únicamente para realizar actividades de tipo laboral y para facilitar las tareas o comunicaciones durante la ejecución de las mismas.

Los dispositivos móviles deben estar registrados en un sistema de información para el control de la tenencia y ubicación de los mismos.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Las aplicaciones que se instalen en los dispositivos móviles serán aquellas autorizadas e instaladas por el área de sistemas o quien tenga la responsabilidad de operación de los mismos.

Los dispositivos móviles deben tener control de acceso de usuario para controlar el acceso no autorizado a los mismos.

La pérdida o extravío de los dispositivos móviles deberá ser reportada inmediatamente y realizar el procedimiento administrativo y legal para el caso.

El uso y buen trato de los dispositivos móviles es responsabilidad de los usuarios a quien se le asigne el dispositivo para desempeño de su labor.

Estos dispositivos de propiedad de la Alcaldía de San antero deben ser conectados a redes autorizadas, no deben ser conectados a redes públicas que permitan la exposición de la información en ellos almacenada.

Responsables:
Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología del ente territorial.

2.3. Seguridad de los Recursos Humanos

2.3.1. Política para la seguridad de los recursos humanos

Objetivo.
Definir el proceso de vinculación del recurso humano de acuerdo a los requisitos exigidos por la MSPI y por la ley de manera que este reglamentado las responsabilidades y roles que se cumplen en el cargo al momento de obtenerlo o asumirlo o dejarlo.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Antes de realizar la vinculación del recurso humano, realizar las verificaciones de idoneidad del candidato al cargo, teniendo en cuenta las normas legales, éticas y a la clasificación y acceso a la información que va a manejar.

Al recurso humano (empleado o contratistas) se le deben establecer sus responsabilidades en los términos y condiciones de empleo al vincularlo, definiéndolos de acuerdo a la seguridad de la información.

Programar y desarrollar capacitaciones periódicas para concientización de la importancia de la seguridad de la Información en el recurso humano vinculado.

Verificar que el recurso humano (empleados y contratistas) están cumpliendo con los procedimientos y políticas definidos y exigidos para el manejo de la seguridad de la información.

Sancionar y aplicar acciones de manera formal al recurso humano que viole los lineamientos definidos en la seguridad de la información.

Al momento de realizar una desvinculación del recurso humano anular todos los perfiles y accesos definidos para el manejo de información del empleado o contratista desvinculado.

Al hacer un cambio de perfiles o responsabilidades del cargo al recurso humano, comunicar los mismos y reasignar los permisos requeridos, sea anulando o creando nuevos.

Responsables:
Alta dirección y funcionarios del nivel Directivo, asesores, Área de Recursos Humanos, Área de tecnología del ente territorial.

2.4. Seguridad de los Activos de Información

2.4.1. Política de Responsabilidad por los Activos de Información

Objetivo.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Establecer los Activos de información y asignar responsabilidades para su manejo y administración.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Establecer la forma en que se puede manejar e identificar los activos de información.

Responsables:
Alta dirección y funcionarios del nivel Directivo, asesores, Área de Recursos Humanos, Área de tecnología del ente territorial.

2.4.1.1. Política de manejo de Activos de Información

Objetivo.
Manejar de manera organizada los activos de información para garantizar la seguridad en su administración.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Definir el sistema bajo el cual la Alcaldía de San antero realizará o manejará el Inventario de Activos de Información.

Realizar el Inventario de Activos de Información incluyendo solo aquellos que pertenecen a la Alcaldía de San Antero.

Establecer las responsabilidades de uso de los activos de información y la información asociada, así como las instalaciones asociadas al procesamiento de la misma.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

El recurso humano (empleado o contratista) que tiene activos de información asignados o bajo su responsabilidad debe devolverlos al momento de terminar su vinculación o cambiar de cargo en la Alcaldía de San antero.

Los activos tecnológicos serán usados de acuerdo a la autorización del área tecnológica y a las asignaciones definidas para ello y la información almacenada en ellos será manejada con responsabilidad del usuario sin posibilidad de hacer copia de información reservada sin previo permiso del superior inmediato.

Los activos de información (aplicaciones, sistemas de información y equipos informáticos) deben ser solicitados al área tecnológica en coordinación con la alta dirección.

Los activos de información de la Alcaldía de San Antero no podrán ser usados para ningún fin ajeno a las actividades laborales en la entidad.

El recurso humano de la Alcaldía de San Antero no debe instalar ni modificar ninguna de los activos de información tecnológicos que procesen o mantengan información (aplicaciones) sin previa autorización del área de tecnología.

Todo usuario es responsable de las acciones asociadas a su credencial de acceso y no podrá acceder usando una credencial ajena a él.

Es responsabilidad del área tecnológica velar por el aseguramiento de las redes y acceso a internet.
Los archivos que provengan de fuentes externas a la Alcaldía de San antero deben ser analizados y revisados por la aplicación de antivirus instalada y reportado cualquier caso de infección o detección de virus.

Responsables:
Alta dirección y funcionarios del nivel Directivo, asesores, Área de Recursos Humanos, Área de tecnología del ente territorial.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

2.4.2. Política de clasificación de Activos de Información

Objetivo.
Manejar de manera organizada y consciente los activos de información que posee la Alcaldía de San antero para brindar un nivel apropiado de protección.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Clasificar los Activos de Información de acuerdo a los requisitos legales, el valor, la criticidad y su susceptibilidad a la divulgación o acceso no autorizado a los mismos.

Realizar una identificación de activos mediante un sistema de etiquetas de acuerdo con la clasificación de los mismos.

El manejo y uso de los activos se establecerá de acuerdo a la clasificación de los mismos y se asignará la responsabilidad de su manejo y administración al recurso humano encargado del área donde repose el activo.

Los activos de información son de propiedad de la Alcaldía de San antero, por tanto, cualquier activo generado en la entidad es propio y debe reposar en la entidad y ser usado exclusivamente por ella de acuerdo a su clasificación.

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

2.4.3. Política de Manejo de medios de Soporte de Información

Objetivo.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Garantizar la salvaguarda de la información de manera que pueda ser protegida de divulgación, modificación o sustracción y eliminación la información almacenada en medios de soporte.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Realizar las salvaguardas de la información en medios y formas que garanticen los principios (disponibilidad, integridad y confidencialidad) de la seguridad de la información almacenada y el acceso controlado para evitar la intrusión a la misma.

Asignar de manera tacita la responsabilidad a quien corresponda realizar y administrar las salvaguardas de la información.

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

2.5. Control de acceso

2.5.1. Política de Control de Acceso

Objetivo.
Garantizar que la información administrada y almacenada en la Alcaldía de San Antero se mantenga disponible para el recurso humano y usuarios con permisos para acceder a ella de acuerdo al grado de confidencialidad definido.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Directrices:
La alcaldía de San Antero Manejará perfiles de acceso definidos de acuerdo a los roles y responsabilidades sobre la información almacenada y de acuerdo a su clasificación.

El recurso humano con acceso y perfiles definidos en los sistemas de información se les asignará una credencial de acceso única, la cual es de uso personal e intransferible

El Recurso humano con credenciales de acceso es responsable del manejo y uso de las mismas.

El área de tecnología es quien está autorizada para instalar cualquier clase de software o aplicaciones en la alcaldía de San antero, en caso de que un tercero lo requiera debe ser autorizado por esta área.

Los usuarios con permisos para acceso remoto tienen definido una ruta de acceso y son responsables por el uso y manejo de la credencial y el acceso a los sistemas de información.

El área de tecnología revisará periódicamente el movimiento de las credenciales de acceso y ajustará los permisos de acceso a los sistemas de información.

La autenticación es secreta y responsabilidad del usuario designado para el rol.

Solo tendrán privilegios de usuario los roles y perfiles necesarios para la administración y operación de los sistemas de Información.

Las contraseñas deben cumplir los requisitos de contraseña segura, tal vez como, longitud mayor a 8 caracteres, con combinaciones alfa numéricas, uso de mayúsculas y minúsculas, caracteres especiales, usar diferentes claves para los servicios y accesos, evitar palabras comunes o de fácil deducción, de modo que se garantice la seguridad de las mismas.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Cambiar periódicamente las contraseñas.

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

2.6. Criptografía

2.6.1. Política de Control Criptográfico

Objetivo.
Garantizar que la información que circula por la red interna o publica viaje encriptada, para evitar acceso no autorizado o intrusiones en los sistemas de información.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Establecer el método de criptografía que se usará en la transmisión o intercambio de datos seguros a través de la red de datos.

Definir el procedimiento para el uso de la herramienta de encriptación, teniendo en cuenta los requisitos exigidos por la ley.

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

2.7. Seguridad Ambiental y Física.

2.7.1. Política para área segura.

Objetivo.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Garantizar el acceso controla a las áreas de procesamiento de información y a los activos de información en la Alcaldía de San Antero para garantizar los principios de la seguridad de la información.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Establecer lineamientos que permitan controlar el acceso físico a las instalaciones de procesamiento de datos y a las instalaciones de la Alcaldía de San antero, para controlar el acceso no autorizado.

Realizar control en las entradas y salidas de las instalaciones de la alcaldía de San Antero, verificar la tenencia y porte de elementos que puedan afectar los activos de la entidad.

Asignar mecanismos que eviten la ocurrencia de fallos en el sistema eléctrico de las instalaciones y centro de datos.

Reducir al mínimo la existencia de material combustible dentro del centro de datos o cableado, evitando ocurrencia de incendios o desastres por elementos que se encuentren en este espacio.

El centro de datos debe constar de todas las medidas de seguridad industriales y de salud ocupacional, sistema de UPS para respaldo, refrigeración adecuada y precisa, alarmas de detección de humo, sistemas automáticos de extinción de fuego, extintores o sistemas contra incendio con la capacidad de evitar fuego por productos electrónicos.

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

2.7.2. Política para la Seguridad en los equipos.

Objetivo.
Evitar la pérdida, daño, robo o compromiso de los activos de información asociados a los dispositivos tecnológicos y la interrupción de la operación en las instalaciones de la Alcaldía de San antero.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Los equipos deben ser ubicados e instalados en áreas protegidas de riesgos y amenazas y accesos no autorizados.

Los equipos deben tener fuentes de suministro de energía de reserva o UPS que les proteja de fallos en la corriente alterna.

El sistema de cableado de potencia y datos debe estar protegido contra interrupciones interferencia o daños.

Los equipos deben contar con un plan de mantenimiento continuo que evite la interrupción y garantice la disponibilidad continua del servicio, el cual debe ser registrado. En su hoja de vida.

Los equipos o activos tecnológicos no deben ser retirados de su sitio de trabajo sin previa autorización del área de tecnología y almacén.

Los equipos que entren en desuso o baja operativa deben ser tratados de Manera segura logrando que cualquier dato confidencial sea eliminado o borrado antes de ser reusado.

Los equipos deben mantenerse con claves de acceso activadas mientras se encuentren sin supervisión.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Los puestos de trabajo deben manejar el escritorio limpio y la pantalla limpia con el fin de garantizar la seguridad de la información y evitar el acceso o manipulación no autorizado.

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

2.8. Seguridad de las operaciones.

2.8.1. Política para la seguridad operacional.

Objetivo.
Garantizar que los procedimientos se realicen de manera segura y correctamente en las instalaciones y áreas de procesamiento de información.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Los procedimientos que realiza el usuario operador deberán estar documentados y ser realizados como se encuentran especificados, y estar disponibles para su consulta por parte del operador.

Las operaciones o procedimientos que sufran cambios deben ser controlados, con el fin de que se garantice la seguridad de la información, la estabilidad y continuidad de las actividades.

Periódicamente se debe realizar una verificación de los recursos tecnológicos y operativos para evaluar la capacidad del desempeño del sistema.

Los cambios que realizar en el ambiente de operaciones deberán ser probados en un ambiente de prueba antes de ser puesto en producción y así reducir riesgos.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

2.8.2. Política para protección contra códigos maliciosos.

Objetivo.
Garantizar que las áreas de procesamiento de información estén protegidas contra software o código malicioso.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
La alcaldía de san Antero contará con mecanismos de protección contra códigos maliciosos que permitan la detección y prevención de los mismos.

Crear un ambiente de concienciación entre los usuarios y su responsabilidad en el manejo y en la seguridad de la información que acceden y manejan en los dispositivos y medios de comunicación.

Mantener copias de respaldo en áreas externas a las instalaciones de la Alcaldía de San antero, como mecanismo de protección de la información almacenada y genera da en los sistemas de información.

Tener un registro de evento o incidentes de seguridad y acciones del usuario con el fin de conocer la sinergia del sistema y revisar el comportamiento.

Los registros deben mantenerse salvaguardados de alteraciones o acceso no autorizado.

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

2.8.3. Política para control de software operacional.

Objetivo.
Garantizar que los sistemas y sistemas de información en operación mantengan la integridad de la información.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Mantener un esquema de operación sobre la administración y operación de equipos, que garantice la operatividad e integridad en el proceso.

El parea de tecnología tiene la responsabilidad de operación y mantenimiento y gestión de vulnerabilidades de los equipos en producción para minimizar así el riesgo.

El área de tecnología es la única encargada de la instalación y manipulación del software operacional instalado en los equipos de cómputo, ningún usuario está autorizado para realizar cambios en los mismos.

Realizar revisiones periódicas sobre los equipos para verificar la alteración sobre el software instalado en los equipos.

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

2.9. Seguridad de las comunicaciones.

2.9.1. Política para la Gestión de Seguridad de las redes

Objetivo.
Garantizar que los sistemas de comunicaciones operen y estén disponibles mediante mecanismos que lo garanticen.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Mantener un esquema de medidas que permita tener disponible los servicios de red y comunicaciones.

Implementar dispositivos de seguridad (firewalls, UTMs, sistema detector de intrusos) que monitoreen la actividad en la red de datos de la Alcaldía de San Antero.

Identificar los servicios y protocolos autorizados y configurados en la red de datos y cerrar los puertos servicios y eliminar protocolos no usados.

Realizar segmentación de red, para hacer un aprovechamiento mejor del ancho de banda.

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

2.9.2. Política para la transferencia de información

Objetivo.
Garantizar que la información que circula en la red interna y externa sea haga de manera segura.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:

Establecer mecanismos y procedimientos que garanticen y protejan de la interceptación y acceso no autorizado de la información transmitida por las redes de datos.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Establecer el procedimiento para la transferencia de información en dispositivos a nivel interno.

Definir y establecer acuerdos de confidencialidad con el recurso humano de acuerdo a la clasificación de la información que maneja y transfiere.

Responsables:
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

2.9.3. Adquisición, Desarrollo y mantenimiento de sistemas de información

Objetivo.
Garantizar que la seguridad de la información se incluya en el proceso del ciclo de vida del sistema de información.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Establecer los requisitos de seguridad que se deben incluir en los sistemas de información nuevos o en operación.

Los servicios de aplicaciones prestados por los sistemas de información sobre redes de datos deben ser protegidos para garantizar los principios de la seguridad de la información.

Establecer que la seguridad de la información está definida para todo el ciclo de visa del desarrollo del sistema de información.

Monitorear los cambios en las aplicaciones críticas y evitar efectos adversos.

Realizar pruebas de funcionalidad de los sistemas de información.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Responsables:
Funcionarios del nivel Directivo, asesores, Área de Tecnología, contratistas, del ente territorial.

2.10. Política para las relaciones con proveedores.

Objetivo.
Garantizar la seguridad de la información que se maneje con os proveedores.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Establecer y firmar acuerdos de confidencialidad para el manejo de información y así mitigar los riesgos asociados al acceso a la información.

Realizar gestión y seguimiento a los servicios prestados por los proveedores, incluido mantenimiento y mejora en las políticas y procedimientos y controles de seguridad.

Responsables:
Funcionarios del nivel Directivo, asesores, Área de Tecnología, contratistas, del ente territorial

2.11. Política para la Gestión de incidentes de Seguridad

Objetivo.
Garantizar el manejo y control en caso de ocurrencia de un incidente de seguridad

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Establecer procedimientos y asignar responsabilidades al recurso humano para el manejo y gestión de los incidentes de seguridad con el fin de garantizar una respuesta rápida, eficiente y ordenada que permita la continuidad de las actividades.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Definir la ruta para el reporte de los eventos o incidentes inmediatamente ocurran y así mismo reporten las debilidades de seguridad observadas.

Evaluar los eventos reportados y valorar si se clasifican como incidentes de seguridad.
El área de tecnología debe dar respuesta a los incidentes de seguridad reportados, de acuerdo con el procedimiento definido.

Usar la experiencia del manejo de los incidentes de seguridad para evitar futuras ocurrencias del mismo tipo.

Responsables:
Funcionarios del nivel Directivo, asesores, Área de Tecnología, contratistas, del ente territorial

2.12. Política para la continuidad del negocio

Objetivo.
Garantizar la continuidad de la seguridad de la información en caso de la ocurrencia de un incidente de seguridad que altere la operación en la Alcaldía de San Antero.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Establecer los requisitos que permitan de manera ordenada la continuidad de las actividades en caso de una situación adversa.

Definir y documentar los procedimientos a realizar para garantizar la seguridad de la información y trabajar por la continuidad de las actividades en caso de una adversidad

Evaluar que los procedimientos y controles definidos son los adecuados para garantizar la continuidad y operación delas actividades en la situación adversa.

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Tener disposición de sitios o instalaciones de procesamiento para la activación de servicios en caso de daño grave y tener la disponibilidad para la reanudación de operaciones.

Responsables:
Funcionarios del nivel Directivo, asesores, Área de Tecnología, contratistas, del ente territorial

2.13. Política para el Cumplimiento

Objetivo.
Garantizar la continuidad de la seguridad de la información en caso de la ocurrencia de un incidente de seguridad que altere la operación en la Alcaldía de San Antero.

Aplicabilidad.
Esta política aplica a la Alta dirección y funcionarios del nivel Directivo, asesores, Área de Tecnología, personal de planta, contratistas, del ente territorial.

Directrices:
Establecer los requisitos que permitan de manera ordenada la continuidad de las actividades en caso de una situación adversa.

Definir y documentar los procedimientos a realizar para garantizar la seguridad de la información y trabajar por la continuidad de las actividades en caso de una adversidad

Evaluar que los procedimientos y controles definidos son los adecuados para garantizar la continuidad y operación delas actividades en la situación adversa.

Tener disposición de sitios o instalaciones de procesamiento para la activación de servicios en caso de daño grave y tener la disponibilidad para la reanudación de operaciones.

Responsables:
Funcionarios del nivel Directivo, asesores, Área de Tecnología, contratistas, del ente territorial

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Referencias

SGS Colombia S.A., División S&SC, VISIÓN GENERAL ISO 27001:2013. (2015). Modelo de seguridad, obtenido de: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Modelo de Seguridad y privacidad de la Información. Elaboración de la política general de seguridad y privacidad de la información obtenido de: http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Elaborado Por	Revisado Por	Aprobado por
Cargo	Cargo	Cargo
Firma	Firma	Firma

Anexo F **REUMEN ANALITICO ESPECIALIZADO R.A.E**

TEMA	Proyecto aplicado para grado especialización en seguridad informática
TÍTULO	DIAGNOSTICO E IMPLEMENTACIÓN DE CONTROLES Y MECANISMOS DE SEGURIDAD EN LA RED DE DATOS DE LA ALCALDÍA DE SAN ANTERO CÓRDOBA
AUTORES	PADILLA GARCES Irina y MOSQUERA ZÚÑIGA Francisco Javier
FUENTES BIBLIOGRÁFICAS	BORTNIK, Sebastián, Universidad Nacional Autónoma de México, Pruebas de Penetracion para principiantes- 5 Herramientas. Obtenido de http://revista.seguridad.unam.mx/numero-18/pruebas-de-penetraci%C3%B3n-para-principiantes-5-herramientas-para-empezar CRATON, Jhon, Home Blog Projects CV Contact, obtenido de https://joncraton.org/blog/46/netcat-for-windows/ MIERES, Jorge, Ataques informáticos, 2009 https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf VERGARA, Kevin, Blog informático, 2016. 12 herramientas de diagnóstico y monitoreo de red, http://www.bloginformatico.com/12-herramientas-de-diagonstico-y-monitoreo-de-redes-axence-nettools.php MARTÍNEZ MOLINA, Kelly Johanna y PACHECO MENESES, Javys y ZÚÑIGA SILGADO, Isaac, (2009), Firewall – Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas y Medianas Empresas), http://revistas.uis.edu.co/index.php/revistauisingenierias/article/view/506/830

AÑO	2018
RESUMEN	Diagnosticar la red telemática de la alcaldía de San Antero y de acuerdo con los resultados implementar controles y mecanismos de seguridad con el fin de proteger la información que se genera en la alcaldía
PALABRAS CLAVES	Sistema de gestión de seguridad de la información, Magerit, ISO 27001, integridad, disponibilidad, confidencialidad, trazabilidad, autenticidad, Alcaldía de San Antero, funcionarios, usuarios, equipos, controles
CONTENIDOS	INTRODUCCIÓN OBJETIVOS PLANTEAMIENTO, DEFINICIÓN Y FORMULACIÓN DEL PROBLEMA JUSTIFICACIÓN ALCANCE Y DELIMITACIÓN DEL PROYECTO MARCO REFERENCIAL, TEÓRICO, CONCEPTUAL, CONTEXTUAL Y LEGAL RECURSOS METODOLOGIA INSTRUMENTOS DESARROLLO DEL PROYECTO CRONOGRAMA CONTINUIDAD DEL NEGOCIO DIVULGACIÓN CONCLUSIONES BIBLIOGRAFÍA ANEXOS
DESCRIPCION DEL PROBLEMA	Debido al desarrollo de proyectos tecnológicos sin esquemas bien diseñados y sin mecanismos y políticas de manejo y uso de buenas prácticas de TI, todas estas carencias tienen expuesta a la entidad a amenazas como: • Ataques de por virus o software malicioso a los sistemas críticos y equipos de cómputo en puestos de trabajo • Perdida de datos en sistemas críticos y en áreas de oficinas.

	• Perdida de información de la entidad por rotación o salida de personal durante el periodo de gobierno o dentro de él. • Mal manejo de los equipos de cómputo y programas u aplicaciones en la red, por parte de los usuarios internos. • Accesos no autorizados a los sistemas de información o las herramientas de TI por actores interno o externos. Los riesgos a que está expuesta la entidad en materia de seguridad informática son variados y en todos los aspectos, la alcaldía carece de mecanismos y políticas de seguridad para la protección de los sistemas, herramientas de TI y para la aplicación de buenas prácticas de TI. De manera tal que puede la entidad quedar en situación de calamidad o desastre ante la ocurrencia de un ataque al sistema de red y cualquier elemento que pertenezca a ella, porque son muchas las puertas de entrada a los sistemas de la entidad, dado la carencia de controles y mecanismos de seguridad establecidos hoy día.
OBJETIVOS	OBJETIVO GENERAL Diagnosticar la seguridad de la red de datos y evaluar los controles y mecanismos a implementar en la alcaldía de San Antero. OBJETIVOS ESPECÍFICOS Levantar información conceptual y estado de arte, métodos, herramientas de diagnóstico de red y controles de seguridad para la red de datos de la alcaldía de san antero. Realizar el diagnóstico del estado actual de seguridad a la red de datos de la Alcaldía de San Antero. Diseñar una propuesta de solución de seguridad a la red de datos, documentación y resultados del proyecto.

METODOLOGÍA	Este trabajo desarrollará un tipo de investigación Descriptiva dado que nos permitirá a través del conocimiento de situaciones y actitudes en el comportamiento de la población objetivo de la investigación describir de manera exacta las actividades, proceso, personas y comportamientos de la red de datos para obtener la caracterización de la realidad en estudio. Mediante la aplicación de un método deductivo, se inferirá con el análisis de los datos particulares recolectados un concepto general del estado de la seguridad de la red de datos de la alcaldía de San Antero Córdoba, para llegar al producto, el diagnóstico del estado actual a través de los datos cuantificables recogidos con herramientas de monitoreo y auditoria informática, que van a permitir llevar una estadística cuantitativa y cualitativa de las vulnerabilidades y los hallazgos encontrados.
PRINCIPALES REFERENTES TEÓRICOS	CISCO, Soluciones De Control Y Contención De Amenazas, Publicaciones, Copyright © 2007 Cisco Systems, Inc. Obtenido de: http://www.cisco.com/c/dam/global/es_es/assets/publicaciones/07-08-cisco-control-contencion-amenazas.pdf EMC^2 RSA, Informe Técnico, Detección y Respuesta ante Amenazas basadas en Inteligencia, 2014, obtenido de https://colombia.emc.com/collateral/white-paper/h1304-intelligence-driven-threat-detection-response-wp.pdf REPOSITORIO UNIVERSIDAD TECNOLÓGICA DE PEREIRA, Facultad de Ingenierías, Vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos de las organizaciones, 2009 obtenido de,

	http://repositorio.utp.edu.co/dspace/bitstream/11059/2734/1/0058R173.pdf
PRINCIPALES REFERENTES CONCEPTUALES	UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, Facultad de Ingeniería, Fundamentos de Criptografía, 2016 http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/13-servicios-y-mecanismos-de-seguridad/132-mecanismos-de-seguridad MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LA COMNICACION TIC DE COLOMBIA. Ley 1273 de 2009 de la protección de la información y de los datos. [Consultado 10 de Mayo de 2015]. Disponible en Internet: www.mintic.gov.co/portal/604/articles-3705_documento.pdf SGS Colombia S.A., División S&SC, VISIÓN GENERAL ISO 27001:2013. (2015). OWASP ZAP Zed Attack Proxy Project [en línea]. [Consultado el 7 de Octubre de 2016]. Disponible en: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
RESULTADOS	De acuerdo a la serie de pruebas realizadas hasta el momento no se han encontrado vulnerabilidades críticas en los equipos rastreados, dando una imagen de que el proceso de filtro está bastante bien configurado, dado que el accesos a la Internet en su mayoría se realiza para el manejo de servicios como el correo electrónico y consultas, sin un grado amplio de transacciones en línea en ambientes interoperables que interactúen y comprometan los servicios y equipos internos directamente durante una transacción, en este sentido se debe enfocar las acciones de mejoramiento del sistema telemático hacia el

	desarrollo e implementación de un SGSI el cual permita hacer una identificación más puntual y detallada que organice e identifique los procesos y procedimientos de las áreas críticas y defina mecanismos de control y políticas de seguridad de la información. Así como el desarrollo integral del recurso humano como elemento importante y vulnerable por omisión o desconocimiento de forma que se pueda llevar y crear un proceso integrado de conocimiento y cultura de seguridad en la entidad. Hasta el punto de que el actor interno respete las políticas, procedimientos y aspectos de seguridad, hasta convertirlo en un hábito y lo apliquen a cada instante en la entidad y porque no en su vida cotidiana.
CONCLUSIONES	En el documento se podrán identificar y encontrar definidos los controles y mecanismos de seguridad que deben ser aplicados para garantizar un ambiente controlado y recomendado según las buenas prácticas de TI, para la red de datos de la alcaldía de San Antero Córdoba. Como resultado de todo lo anterior se pretende que la entidad posea un instrumento o herramienta guía para tener en cuenta y mejore sus procesos a través de la retroalimentación de conceptos y pruebas que se dejaran de base para crear conciencia de la importancia de invertir y asumir medidas que puedan subsanar las debilidades y potenciar a la entidad para cumplir con el logro de objetivos operativos y estratégicos en el área de TI y como consecuencia el área de gestión Estratégica.